جامعة الرباط الوطني

كلية الدراسات العليا والبحث العلمي

حجية الأدله التقنية في الجرائم الالكترونية

الفترة من (2011م–2014م)

بحث مقدم لنيل درجة الدكتوراه في العلوم الجنائية والأمنية

إعداد:

معمر علي أبراهيم محمد

إشراف:

أ. الدكتور محمد أحمد أونور

2014م–1435هـ


بسم الله الرحمن الرحيم

لجنة المناقشة

الصفة	الاسم	الجهة	
بروف	عثمان أحمد عثمان	عميد كلية القانون جامعة الرباط الوطني	ممتحن دأخلي
بروف .لواء ركن	عمر عبد الماجد سيد أحمد	معهد الامن الوطني	ممتحن خارجي
أ.مشارك دكتور	محمد أحمد أونور	جامعة الرباط الوطني	مشرف

ألأستهلال

(وَمَا أُوتِيتُم مِّنَ الْعِلْمِ إِلَّا قَلِيلًا)

صدق الله العظيم

الاسراء الاية(85)

الإهداء

اِلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك ولا تطيب

اللحظات إلا بذكرك ولا تطيب الآخرة إلا بعفوك ولا تطيب الجنة إلا برؤيتك

الله جل جلالة

إلي من بلغ الرسالة وأدي الأمانة ونصح الأمة إلي نبي الرحمة ونور العالمين

سيدنا محمد صلي الله علية وسلم

إلى من نهلتُ من معين حُبِّها الذي لا ينضب فارتويت حتى استويت
(أمي الحبيبة)

إلي من كلله الله بالهيبة والوقار إلي من احمل أسمة بكل افتخار إلي من علمني العطاء بدون انتظار والي من علمني ان اتبع النور في الظلام حتى ولو كان ضئيلا

(والدي العزيز)

(أصدقائي وزملائي)

شكر وتقدير

الحمد لله رب العالمين، الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على المبعوث رحمة للعالمين، وعلى آله وصحبه أجمعين وبعد.

إن الله عز وجل أنعم علي نعما كثيرة يعجز اللسان أن يعبر عنها أو يشكر، فالحمد لله على ذلك، وإني والله لأستحي من الله سبحانه وتعالى لما يسدل علي من النعم التي لا تكاد تنتهي إلا وأسدل أخريات نعمة فوق نعمة مع كثرة معاصي ومخالفتي لأمره تبارك وتعالى، لكنه الرحمن الرحيم سبحانه وتعالى ما أعظمه جل جلاله فله الشكر والحمد أولاً وأخيراً وأسأله وهو الكريم المنان أن يعفو ويتجاوز عني إنه هو الجواد الكريم الغفور الرحيم.

ثم إني أتقدم بفائق الشكر والتقدير **لجامعة الرباط الوطني** الممثلة في كلية الدراسات العليا والشكر موصول إلي مشرفي **الدكتور محمد أحمد أونور** الذي فتح لي قلبه وعقله قبل أن يشرف على هذه الرسالة واستفدت منه علماً وأخلاقاً وبسط لي من الكرم ما أعجز عن وصفه فجزاه الله عني خير الجزاء.

والشكر الي سعادة البروفيسور عثمان أحمد عثمان عميد كلية القانون جامعة الرباط الوطني والشكر الي سعادة اللواء الركن بروفيسور عمر عبد الماجد سيد أحمد والشكر للدكتور أحمد الماحي مسجل كلية الدراسات العليا عن أسرة الكلية والشكر لاكاديمية الشرطة العليا ومعهد البحوث الجنائية .

المستخلص

تعد هذه الدراسة من الدراسات الوصفية بعنوان حجية الأدله التقنية في الجرائم الالكترونية من العام (2011–2014) وذلك لتزايد ادراك المجتمع الدولي بخطورة الجريمه بتطوراتها السريعه التى املتها ظروف العصر وكانت مشكلة البحث متمثلة في نقطتين في موضوع الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت وخاصة جرائم الارهاب الالكتروني وحجية اثباتها جنائياً النقطة الأولى وهي ضعف المعلومات العامة حول هذا الموضوع لدى عدد كبير من رجال القانون غير المختصين في مثل هذا الموضوع النقطة الثانية في هذه الدراسة هي تسليط الضوء على جريمة الارهاب الالكتروني ودليل إثباتها نظراً لإهميتها وموقف النصوص القائمة في القانون الجنائي السوداني ، حول مدى انطباقه على مثل هذه الجريمة مع دراسة المعاهدات والاتفاقيات الدولية في شأن مكافحة هذه الجريمة وجاءت أهمية الدراسة تظهر أهمية هذا البحث في الدور الذي تلعبه وسائل الاتصال الاجتماعى ومدى تأثيرها على مظاهر الحياة في جميع مجالاتها. ومدى الحاجة لبحث مايعتريها من مشكلات قانونية قد تقف عقبه أمامها ومحاولة تذليلها وإيجاد الحلول القانونية المناسبة لها وذلك على اعتبار ان التكنولوجيا والقانون متلازمان وكانت أهداف الدراسة هي إلقاء الضوء على الجرائم الالكترونية من ناحية عامه وجرائم الارهاب الالكتروني من ناحية خاصة فضلاً عن إيجاد طرق لإثبات الجرائم إثباتاً كجرائم غير تقليدية واستخدام التقنية الحديثه فى الاثبات الجنائى وايجاد سند قانونى لقبول البينات التى تستخدم فيها التقنيات الحديثه وأتي البحث بعدة نتائج وتوصيات تمثل إضافة حقيقية في مجال القانون والجرائم الالكترونية والادله التقنية وجاءت أهم النتائج كشف هذا النوع من الجرائم وإثباتها ليس بالشئ السهل وانما يستلزم استخدام تقنيات حديثة في عمليات التحرى والكشف عن الأدلة والتحقيق لأجل ذلك يمكن إستخراج تقنية المعلومات بشكل دائم كوسيلة من وسائل ضبط الجريمة والتحقق فيها و ما من دول يمكنها النجاح في مواجهة هذه الانماط المستحدثة بمفردها دون تعاون وتنسيق

مع غيرها في الدول سواء في مجال المساعدات القضائية المتبادلة أوفي مجال تسليم المجرمين أو في مجال التدريب وكانت وأهم التوصيات وضع برامج حماية كافية من الاختراق والتدمير لمؤسسات الدوله الحيويه التى تستخدم التقنيات الحديثه والعمل على التحديث المستمر لهذه البرامج لتقوم بالتنبيه عند حدوث اى اختراق و ضرورة التعاون بين الدول فى انشاء مراكز وطنية تهتم بقضايا الارهاب الالكترونى والجرائم الالكترونيه التى اكتسحت عالم الانترنت والتقنية ودراستها من النواحى التشريعيه وبيان اثرها السياسى والاقتصادى والاجتماعى .

Abstract

This is a study of descriptive studies entitled authoritative technical manuals in electronic public crimes (2011-2014) in order to increase awareness of the international community the seriousness of the crime Food Pttoradtha dictated by age conditions were research problem represented by two points on the subject of crimes resulting from the illegal use of the Internet and private terrorism-mail crimes and Authentic provable criminal first point which is twice the general information about the subject of a large number of men of law is competent in such a topic the second point in this study is to shed light on the crime of terrorism-mail and evidence to prove because of its importance and the position of the existing texts in Sudanese criminal law , about how it applies to such a crime with the study of international treaties and conventions on combating this crime came importance of the study show the importance of this research in the role played by the means of social communication and its impact on all aspects of life in the fields. And the need to discuss Mayatrea of legal problems might obstacle in front of her and try to overcome them and to find the appropriate legal solutions to them and so on the grounds that the technology and the law are inseparable The objectives of the study is to shed light on the electronic crimes in terms of general crimes cyber terrorism, especially the one hand, as well as finding ways to prove the crimes WITNESS crimes unconventional use of modern technology in proof of criminal and find a legal basis for admission of evidence that use of modern technologies and brought Find several findings and recommendations represent a real addition in the field of law and crimes electronic technical manuals came the most important results revealed this type of crime and prove not Bci easy, but requires the use of techniques modern in the investigation and disclosure of evidence and the investigation for that can extract information technology permanently as a

means of crime control and check where and what countries can succeed in the face of these patterns developed on its own without the cooperation and coordination with others in the States, whether in the field of judicial mutual assistance or in the field extradition or in training and was the most important recommendations put adequate protection from penetration and destruction of state institutions vitality that uses modern technology programs and work on the continuous updating of these programs to the alarm in case of any breach and the need for cooperation between countries to establish national centers concerned with the issues of cyber terrorism and cyber crime that has swept the online world, technical and studied aspects of the legislative and political impact statement, economic and social.

قائمة المحتويات

الإطار المنهجي للبحث

الفصل الثاني

الارهاب الالكتروني

المبحث الأول: ماهية الارهاب

المبحث الثاني: القضاء على الإرهاب الإلكتروني

المبحث الثالث: جرائم التجسس الإلكتروني

الفصل الأول

الجرائم الالكترونية

المبحث الأول: الأدلة الجنائية

المبحث الثاني: جرائم الانترنت

المبحث الثالث: مكافحة جرائم الانترنت

الفصل الثالث

الدليل الإلكترونى

المبحث الأول: الدليل الالكتروني

المبحث الثاني: قواعد الإثبــات الالكتروني

المبحث الثالث: شروط الدليل الإلكتروني المستمد من التفتيش

الفصل الرابع

الخبرة في الجرائم الالكترونية

المبحث الأول: الخبرة في الجرائم الالكترونية

المبحث الثاني: شروط صحة اعمال الخبرة الفنية ومدى حجيتها

المبحث الثالث : بينة الخبير في الجرائم الالكترونية

الخاتمة

أولاً: النتائج

ثانياً: التوصيات

قائمة المراجع والمصادر

الملاحق

الإطار المنهجي للخطة والدراسات السابقة

1- ألمقدمة :

في هذا العصر عصر تكنولوجيا المعلومات أصبح ارتكاب الجرائم يعتمد بقدر كبير جداً على التقنيات الحديثة نسبة لدقتها وصعوبة التوصل الى مرتكبيها علاوة على انها جرائم عابرة للحدود ويمكن التحكم فيها عن بعد مما يجعل منها طريقة مقبولة لمرتكبى هذه الجرائم لاستخدامها ، هذه الدقة مكنت من استخدام هذه التقنيات الحديثة فى الكشف عن هذه الجرائم وذلك باستخدام نفس التقنيات للكشف عن مرتكبى الجرائم الامر الذى يتطلب الاتجاه لسن تشريعات تدعم الدليل المستمد من هذه التقنيات مما جعل بعض الدول تجرى تعديلات جزرية على قوانينها وسن تشريعات جديدة حتى تجعل من هذه الادلة مقبولة امام المحاكم.

الزيادة في الجرائم الالكترونية وأتجاه نسبة كبيرة من فئات المجتمعات لارتكابها لعدة دوافع اصبح مهدداً للأَمن الاجتماعي والاقتصادي والسياسي للدول وهذه الجرائم مثل التجسس والارهاب والتحريض السياسي، هذا فضلا عن التدريب على وسائل حديثة وطرق غامضة تجعل الوصول لمرتكبى مثل هذه الجرائم صعباً فى ظل انها عابرةُ للحدود وتحتاج الى أتفاقيات محددةُ لتبادل المجرمينٍ وكل مايختص بالتعاون الدولي فى هذا الشأن، كما ان هذا الواقع إقتضى إعداد العدة لمكافحة هذا النوع من الجرائم بكل السبل والوسائل الفنية والتقنية بإعداد الكوادر المؤهلة والمدربة للكشف عنها . وكذلك الاهتمام بالناحية التشريعية والقانونية في المكافحة مع وضع وزن قانوني للدليل الالكتروني جنائياً. كما ان الاثبات الجنائي بالادلة التقنية من أبرز تطورات العصر الحديث في كافة النظم القانونية ، كذلك الفكر الاجرامي قد تطور باستخدامة لهذة الوسائل واصبح الاثبات صعبا على القائمين على المكافحة ، وهذا الواقع يتطلب من المؤسسات التشريعية أن تستحدث من التشريعات في ما يلائم

هذا النوع من الجرائم فضلاً على إنشاء أجهزة فنية متخصصة في الاثبات العلمي الفني لهذه الجرائم.

ولقد تزايد ادراك المجتمع الدولي بخطورة الجريمه بتطوراتها السريعه التى املتها ظروف العصر. وتصاعد قلقة ازاء صورها المستحدثه التى ارتدت ثوبا دوليا جديداً فى وسائل ارتكابها ، حيث لم تعُد الحدود الوطنيه الان عائقا لها بل تجاوزتها لتصبح عبر وطنيه ، بل وعبر أقليميه وعبر قاريه .

هذا ولقد انصب أهتمام المجتمع الدولي خلال الاونهُ الاخيره على ضرورة التغلب على الصعاب والتحديات التى فرضتها الجريمة المعاصرة، وصورها المستحدثه ومكافحتها بفعاليه والتعاون من أجل منع كافة أشكالها، وذلك من خلال تصعيد اسهامات منظماته والتعاون بين هيئاته الدوليه المعنيه فى هذا المجال وبالتنسيق مع سائر الدول التى لا تستطيع بمفردها مواجهة هذا النوع من الاجرام الحديث العابر للحدود، وذلك مع استصحاب دخول محور المعلومات والتقانة ضمن المحاور الرئيسه فى عملية التخطيط لتحقيق الامن القومي والمتمثله فى السياسه الاقتصادية والاعلام والامن والاجتماع علاوة على المعلومات والحوسبه والتقانة.

2- مشكلة البحث:

لا أحد ينكر ان موضوع الجرائم الالكترونية او جرائم الانترنت هي من المواضيع الحديثة كلياً فأن البحث فيها لا يخلو من الصعوبات فعالم الانترنت عالم متجدد ومتغير باستمرار وينمو بشكل كبير وواسع ويحتوى على كم هائل من الرموز الاجنبية والمصطلحات العلمية الكثيرة والتي تحتاج الى شخص متخصص في هذا المجال لمعرفة المقصود بها ناهيك عن علاقة موضوع الدراسة والتي تعتبر من المواضيع الجديدة نسبياً بالنسبة للدراسات الجنائية كل هذه الامور تصعب على الباحث مهمته .

من خلال ذلك استوقفتني نقطتين في موضوع الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت وخاصة جرائم الارهاب الالكتروني وحجية اثباتها جنائياً :-

النقطة الأولى :-

وهي ضعف المعلومات العامة حول هذا الموضوع لدى عدد كبير من رجال القانون غير المختصين في مثل هذا الموضوع ، على اعتبارانه من المواضيع الحديثة .هذا بجانب ندرة المصادر والمراجع التى تتناول هذا الموضوع وذلك لحداثته ودقة مفاهيمه بالاضافه الى الحصار المفروض فى مجال البرمجيات مما كان له الاثر الكبير فى الحصول على المعلومة وتطبيقها تقنيا.

النقطة الثانية :-

لم نتوصل الى دراسة حديثة تناولت هذا الموضوع طبقاً للقانون الجنائي أو العقوبات في الدول التي تسمى ذلك ، الأمر الذي حدا بنا الى أن نتناول هذا الموضوع بشكل مبسط ،بعيداً عن التعقيد حتى يفهمه القارئ العادي قبل القانوني. وسنحاول في هذه الدراسة تسليط الضوء على جريمة الارهاب الالكتروني ودليل إثباتها نظراً لإهميتها وموقف النصوص القائمة في القانون الجنائي السوداني ، حول مدى انطباقه على مثل هذه الجريمة مع دراسة المعاهدات والاتفاقيات الدولية في شأن مكافحة هذه الجريمة. وكان لابد لنا قبل الحديث عن الجريمة الالكترونية والارهاب الالكتروني أن نلقى نظرة على جرائم الانترنت وتعريفها وبيان سماتها وانواع هذه الجرائم كتمهيد للدخول في هذه الدراسة.

3- أهميـة البـحـث:

تظهر أهمية هذا البحث في الدور الذي تلعبه وسائل الاتصال الاجتماعى ومدى تأثيرها على مظاهر الحياة في جميع مجالاتها. ومدى الحاجة لبحث مايعتريها من مشكلات قانونية قد تقف عقبه أمامها ومحاولة تذليلها وإيجاد الحلول القانونية المناسبة لها وذلك على اعتبار ان التكنولوجيا والقانون متلازمان وكل منهما يخدم الأخر كما تبرز أهمية البحث في موضوع الجرائم الالكترونية عن الاستخدام غير المشروع لشبكة الانترنت في الوقوف على هذه الجريمة الحديثة والتي ظهرت بعد ظهور هذه التقنية التي تخطت جميع المبادئ والأسس القانونية التي كانت سائدة وظهرت على السطح جرائم لم تكن موجودة في السابق كما ظهرت طرق حديثة لارتكاب الجرائم التقليدية. لذلك اصبح من المهم البحث في كيفية مواجهة هذه الجرائم من خلال تطبيق النص القائم دون القياس أو الإخلال بمبدأ الشرعية الجنائية مع الالتزام بقواعد الاثبات والدليل الموثوق الذى يجب أن يتم التوافق عليه .

تكمن أهمية البحث أيضاً في تقديم دراسة نظرية وعملية عن الارهاب الالكتروني ومخاطرة وعن كيفية تقديم دليل عملى لاثبات واقعه الارهاب الالكتروني جنائياً ، وذلك قياساً لما هو موجود في قواعد الاثبات في الجرائم الجنائية الأخرى التقليدية.

لذلك فان هذه الدراسة تركز على العلاقة بين التقنية والإرهاب إجراما ومكافحه وتوضح أن مجتمع تقانة المعلومات قد صنع من العالم قرية صغيره وأن الإرهاب أصبح يهدد العالم وحياة الأبرياء وأصبح يستخدم أشكالا غير مالوفه ومستحدثه مستفيدا من التقنيات الالكترونية المتطورة لتنفيذ عملياته حيث إن تتبعها والوصول إلى مصادرها يكون صعبا لذلك أصبحت ملاذاً أمناً لاستخدامها في العمليات الارهابيه فضلا عن أن مسارحها غير منتظمة وقد تتعدد مما يصعب تتبعها والوصول إليها وذلك باستخدام اطر الأمن السيبرانى او التقنيات الحديثه .وتكتسب هذه الدراسة أهميتها في انها توضح مفهوم ووسائل وأهداف الجريمة الارهابيه الالكترونية كما تأتى

أهمية هذا البحث بمعرفة اثر جريمة الإرهاب التى تستخدم التقنية الحديثه على الامن القومى للدول.

4-أهداف البحث:

من أهداف البحث تحقيق الأتي :-

إلقاء الضوء على الجرائم الالكترونية من ناحية عامه وجرائم الارهاب الالكتروني من ناحية خاصة فضلاً عن إيجاد طرق لإثبات الجرائم إثباتاً كجرائم غير تقليدية واستخدام التقنية الحديثه فى الاثبات الجنائى وايجاد سند قانونى لقبول البينات التى تستخدم فيها التقنيات الحديثه.

5- فرضيات البحث:

الفرضية الاولي : الجرائم الالكترونية عامة والارهاب الالكتروني بصفة خاصة من الجرائم الحديثة والخطيرة التي اصبحت تهدد الامن القومي والاقتصاد الوطني والحياة الاجتماعية .

الفرضية الثانية : هنالك صعوبة في إثبات الجرائم الالكترونية لحداثتها واختلاف قواعد إثباتها عن الجرائم التقليدية .

الفرضية الثالثة: الحوجة ماسة لتشريع جديد يتماشى مع الدليل الالكتروني ومدى إثباته وفق قواعد إثبات جديدة .

الفرضية الرابعة: إساءة إستخدام النظم الحاسوبية وشبكات الاتصال تؤدى الى زيادة معدل الاجرام المعلوماتي .

الفرضية الخامسة : عدم كفاية النظم والقواعد القانونية التقليدية لعملية الاثبات الجنائي للجرائم المعلوماتية .

الفرضية السادسة : قبول الدليل المستمد من استخدام التقنيات الحديثه يعتبر نقله نوعية فى الاثبات.

6-منهج البحث:

إعتمد الباحث في هذه الدراسة على المنهج التحليلى والوصفى التحليلى مع أستصحاب المنهج الاستقرائى للوصول لأهم النتائج التى تحقق استيفاء شروط الادلة التقنية فى الجرائم المعلوماتية وحجيتها فى الاثبات الجنائى.

7-**حدود البحث:**

تنقسم الحدود عادة الى حدود زمانية ومكانية ولاغراض هذا البحث تتمثل الحدود المكانية فى جمهورية السودان منطقياً وكل مواقع دوائر الادلة الجنائية.

الحدود الزمانية تبدا فى سنة 2011م حتى عام 2014م تاريخ مناقشة البحث.

8- طرق جمع المعلومات:

- الكتب والدوريات .
- الوثائق الرسمية والمكاتبات.
- الكتابات السابقة.
- المقابلات.
- الشبكه العنكبوتية.
- القوانين الجنائية السودانية والدولية.
- مشاركات الباحث فى امن المعلومات.

9-دراسات سابقة:

هناك العديد من الدراسات السابقة في هذا المجال سواء اكان على المستوى العربي او على المستوي الاجنبي وفي الاسطر القادمة سوف نسلط الضوء على بعضها :

دراسة د.علي محمود علي حموده

استاذ القانون الجنائي المساعد – كلية الحقوق – جامعة حلوان:

المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكاديمية شرطة دبي ، مركز البحوث والدراسات رقم العدد : 1 السنة : 2003تاريخ الإنعقاد: 26 نيسان 2003تاريخ الإنتهاء: 28 نيسان 2003 الدولة : دبي – الامارات العربية المتحدة بعنوان الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي وتتحدث الرساله عن ان هذه الجرائم قد تتعدى حدود المكان ويصعب بالنسبة لها حساب الزمان. وتحدثت الدراسة بانه ان كانت القوانين العقابية المطبقة قد ضاقت نصوصها بما رحبت عن استيعاب الانواع الجديدة من الجرائم التي جاءت بها ثورة المعلومات من بعد، وان القوانين الاجرائية ليست بأسعد حظا منها لانها ستكون أمام جرائم ترتكب وقد يفر مرتكبها من العقاب مما يلحق اشد الضرر بالمجتمع وبالافراد، كما ان هذه القوانين الاخيرة ستواجهها مشكلات عديدة تتطلب حلولا قانونية قد تكون في منتهى الصعوبة خاصة فيما يتعلق بمسألة الدليل.

دراسة الدكتورجميل عبدالباقي الصغير دار النهضه العربية القاهرة.

عنوانها "الانترنت والقانون الجنائي" ومحورهذه الدراسة حول الاحكام الموضوعية للجرائم المتعلقة بالانترنت والمسئولية الجنائية على تلك الجرائم وتعرض المؤلف فيها الى القانون الفرنسي ومدى إمكانية تطبيق القانون المصري على تلك الجرائم.

دراسة عبدالرحمن محمد بحر العام الدراسى 1420هـ اكاديمية نايف :

عنوانها "معوقات التحقيق في جرائم الانترنت "وهي من الدراسات المسحية ، حيث تم إجراؤها على عينة من ضباط الشرطة بمملكةالبحرين بهدف الكشف عن معوقات التحقيق في هذا النوع من الجرائم بوجه عام ،ولخصت أهم نتائج هذه الدراسة في أن المعوقات الشخصية تمثل عائقاً للتحقيق في جرائم الانترنت لدى 63.3% من عينة الدراسة في حين أجمع أكثر من ثلثي العينة على ان المعوقات الفنية والادارية تمثل عائقاً امام التحقيق في تلك الجرائم وتمثل المعوقات التشريعية عائقاً للتحقيق في هذه الجرائم لدى ربع العينة ،واظهرت نتائج الدراسة أن من أبرز المعوقات الشخصية لدى ضباط الشرطة عدم متابعة المستجدات في مجال جرائم الانترنت كما اظهرت الدراسة ايضاً وجود العديد من المعوقات الفنية كمعوق عدم كفاية المعرفة لاستخدام الحاسب الالي وشبكة الانترنت ومعوق عدم كفاية المعرفة بمصطلحات الحاسب الالي وشبكة الانترنت ومعوق عدم كفاية المعرفة لأساليب ارتكاب جرائم الانترنت ،واظهرت النتائج ايضاً وجود معوقات ادارية كنقص الدورات التخصصية في مجال التحقيق في جرائم الانترنت وعدم توفر خدمة الاتصال بالانترنت أيضاً اظهرت النتائج وجود بعض المعوقات التشريعية كعدم كفاية التشريعات الدولية والمحلية وعدم المعرفة بالتشريعات إن وجدت لدى ضباط الشرطة.

دراسة الدكتور مدحت رمضان 2000م :

عنوانها "جرائم الاعتداء على الاشخاص والانترنت" وهي عبارة عن دراسة قانونية لبعض الأنماط الحديثة من الجرائم الناتجة عن استخدام الانترنت بواسطة الحاسب الالي تعرض فيها المؤلف الي القانون الفرنسي والقانون الامريكي ومدى امكانية استيعاب القانون المصري لتلك الافعال من حيث المكان والاختصاص القضائي كما تتطرق الي المسئولية الجنائية عن جرائم الانترنت ومسئولية موزعي خدمة الانترنت في ذلك.

دراسة الدكتور محمد الامين البشري 1421هـ :

عنوانها " التحقيق في جرائم الحاسب الالي والانترنت " أوضح المؤلف من خلالها خبرات ومعارف الاشخاص والجهات المناط اليه التعامل مع الجريمة سواء المحققون أو موظفو الادعاء العام أو قضاة المحاكم في التعامل مع جرائم الانترنت . ولقد توصل المؤلف من خلال هذه الدراسة الي وضع قواعد عامة للتحقيق في جرائم الانترنت يمكن أن يسترشد بها من قبل المتخصصين والمسئولين عن التعامل مع مثل هذه الجرائم.

دراسة طوني ميشال عيسى 2001م :

عنوانها " التنظيم القانوني لشبكة الانترنت " حاول المؤلف من خلالها إبراز أهم الاشكاليات والصعوبات التي تطرحها شبكة الانترنت وحماية الحقوق الشخصية والأنظمة المعلوماتية على شبكة الانترنت بالاضافة الي بحث الجوانب القانونية التي تثيرها التجارة الالكترونية في شبكة الانترنت كما تطرق المؤلف فيها الي التنظيم القانوني للإشكاليات الدولية في شبكة الانترنت .

دراسة محمد الشوابكة 2002م :

عنوانها " جرائم الحاسوب والانترنت " تمحورت هذه الدراسة حول الجرائم المرتكبة عبر شبكة الانترنت كأداة ايجابية او سلبية للمجرم المعلوماتي وذكرت الدراسة ان شبكة الانترنت عندما تكون أداة ايجابية فهي تسهل للمجرم المعلوماتي ارتكاب جرائم أخري معاقب عليها واظهرت الدراسة ان اغلب جرائم الاعتداء علي الاشخاص المتصور وقوعها علي شبكة الانترنت تقع في هذه الصورة ،أما عندما تكون أداة سلبية فتكون هي هدف الجاني وغايته وذلك بالحصول على البيانات والمعلومات المنقولة عبرها والافادة منها. كما هو الحال في أغلب جرائم الاعتداء على الاموال

وعلى النظم المعلوماتية ، واظهرت الدراسة أن ثمة صعوبات قانونية شتى في تطبيق النصوص القانونية على الانماط المستحدثة من الجرائم ، كما يوجد قصور في قواعد الاجرءات الجنائية التقليدية في مواجهة الاجرام المعلوماتي ،ومن اهم التوصيات التي تمخضت عن هذه الدراسة تلك الخاصة باتخاذ التدابير اللازمة لحل مشكلات الاختصاص القانوني والقضائي بالنسبة لجرائم الانترنت وضرورة تكاتف الجهود الدولية وتوافق السياسات الجنائية في مواجهة هذه الظاهرة .

دراسة محمد عبدالله المنشاوي 2003م :

عنوانها " جرائم الانترنت في المجتمع السعودي" وهي عبارة عن دراسة تطبيقية هدف المؤلف من خلالها الكشف عن حجم ونمط أكثر وأشهر الجرائم المرتكبة عبر شبكة الانترنت في المجتمع السعودي كالجرائم الجنسية والممارسات غير الاخلاقية وجرائم الاختراقات والجرائم المالية وجرائم المواقع المعاديه وجرائم القرصنة الأكثر شيوعاً وتحديد أهم سمات وخصائص مرتكبيها .

دراسة سليمان مهجع العنزي 2003م :

عنوانها "وسائل التحقيق في جرائم نظم المعلومات" تمحورت هذه الدراسة حول السياسة الامنية الشاملة لحماية نظم المعلومات وتحديد أنماط جرائم نظم المعلومات ومدى حدوثها بالمؤسسات واضرارها ودوافعها وحصر الاساليب المستخدمة في ارتكاب جرائم نظم المعلومات ، وبيان العوائق التي تحول دون استخدام تلك الوسائل بالاضافة الي تحديد انواع الادلة المثبته لارتكاب جرائم المعلومات .

دراسة الدكتور :عمر محمد أبو بكر يونس 2004م :

عنوانها "الجرائم الناشئة عن استخدام شبكة الانترنت " تمحورت حول العلاقة القائمة في التشريعات المقارنه بين الانترنت وبين القانون الجنائي سواء من الناحية الموضوعية أو الإجرائية .

دراسة الاستاذ ريد هايلي:

حول فيروسات شبكة الانترنت The Internets Liness : Viruses حول الفيروسات والمعنونة بعنوان واضح ومن خلالها المقصود بالفيروسات وتصنيفها وانواعها المختلفة بالاضافة الي طرق عملها والخسائر التي تسببها .

دراسة الأستاذ أدست:

حول المواقع الاباحية والمعنونة بعنوان Internet Pornography Addiction وهي تبحث مسألة إدمان المواقع الاباحية على شبكة الانترنت بين الباحث من خلالها ان هذا الادمان يرجع الي اسباب نفسية عدة، كذلك اوضح الباحث من خلال الدراسة ان المواقع الاباحية اصبحت مشكلة حقيقية وان الأثار المدمرة لهذة المواقع لا تقتصر على مجتمع دون أخر ومن جهة اخري بين الباحث الاثار السلبية لها والمتمثلة في جرائم الاغتصاب بصفة عامة واغتصاب الاطفال بصفة خاصة والعنف الجنسي وامتهان النساء .

دراسة جلابوكسي وسميث:

حول الجرائم الرقمية " Crime in the Digital Age" بعنوان الانترنت السلبي والمتمثل في نشر الجريمة بأنماط جديدة لم تكن مألوفة في السباق مثل : جرائم غسيل الاموال كذلك وضحت الدراسة الدور الايجابي للانترنت المتمثل في امكانية

استفادة الجهات الامنية من الخدمات التي تقدمها شبكة الانترنت لتسريع إجراءاتها وتحديث أساليبها وتنمية قدرات منتسبيها .

10- هيكل البحث :

يتكون البحث من أطار منهجي ،اربعة فصول وخاتمة والفصل الاول يشمل الجرائم الالكترونية المبحث الاول الأدلة الجنائية المبحث الثاني: جرائم الانترنت المبحث الثالث مكافحة جرائم الانترنت الفصل الثاني يتضمن الارهاب الالكتروني المبحث الأول ماهية الارهاب المبحث الثاني القضاء على الإرهاب الإلكتروني المبحث الثالث جرائم التجسس الإلكتروني أما الفصل الثالث الدليل الإلكترونى المبحث الأول الدليل الالكتروني المبحث الثاني قواعد الإثبات الالكتروني المبحث الثالث شروط الدليل الإلكتروني المستمد من التفتيش الفصل الرابع الخبرة في الجرائم الالكترونية المبحث الأول الخبرة في الجرائم الالكترونية المبحث الثاني شروط صحة اعمال الخبرة الفنية ومدى حجيتها المبحث الثالث بينة الخبير في الجرائم الالكترونية ويحتوي علي الخاتمة

الفصل الاول

المبحث الاول : الأدلة الجنائية

البيّنات لغة جمع بيّنة، وهي الدليل والحجة، وهي اسم لكل ما يبين الحق ويظهره، ويراد بها في القانون إقامة الحجة والدليل أمام القضاء بالطرق التي حددها لإثبات حق أو واقعة تترتب عليها آثار قانونية.[1]

وتحتل البيّنات ووسائل الإثبات أهمية كبيرة، إذ يتوقف عليها الفصل في الخصومات، ورد الحقوق إلى أصحابها، وإقامة العدالة، ومنع العدوان، وتأديب الجناة والمجرمين، لأن القاضي يستحيل عليه الإحاطة بجميع الحوادث والوقائع بنفسه، لذلك يستعين بالأدلة والحجج والبينات. يقع عبء الإثبات في الأصل على عاتق المدعي، ويكتفي المدعى عليه بالإنكار واليمين، ولا يكلَّف الإثباتَ تطبيقاً لقاعدة (البينة على من ادعى ، واليمين على من أنكر) وقد ينقلب عبء الإثبات فيصير على المدعى عليه، كما إذا تقدم المدعى عليه بدفع لدعوى المدعي، فعليه إثبات الوقائع التي تؤيد هذا الدفع، مثل إذا أثبت المدعي دينه [2]

عند المدعى عليه، فادعى الأخير البراءة من الدين، فعليه البينة على ذلك، لأنه صار في الواقع مدعياً للبراءة. وقد يعفي الشرع أو القانون المدعي من عبء الإثبات، ويجعله على المدعى عليه في بعض الحالات، كالمدعى عليه المكلف بالرقابة على القاصر إذا صدر منه ضرر، فعلى الولي أو الوصي أن يثبت أنه قام بواجب الحفظ والعناية الكافية. وعليه الإثبات بأنه قام بواجبه، أو وقع الضرر بسبب خارج عن يده وقواعد عبء الإثبات ليست من النظام العام، ويجوز الاتفاق بين الطرفين على مخالفتها، كالاتفاق بين المؤجر والمستأجر على تحمل المؤجر إثبات

---

[1] مختار الصحاح ، للامام : محمد بن أبي بكر بن عبد القادر الرازي ، (القاهرة : مطبعة دار الجيل ، ب ، ن) ، ص 29.
[2] نفس المرجع السابق ذكره ، ص 30.

حريق الماجوروبلعب الدليل الجنائي دورا مهما في الإثبات الجنائي ويحتل ركناً مهما في السياسة الجنائية وهذه السياسة ترتكز على الشخص المتهم بالإضافة إلى العناية به ،وهو وسيلة تقديرية يمارس من خلاله القاضي سلطته التقديرية ليصل إلى التقدير القانوني السليم للجريمة ونجد أن القاضي يلعب دورا ايجابيا في استقصاء الأدلة للوصول إلى الحقيقة ونجد أن سلطة القاضي التقديرية تختلف باختلاف نظم الإثبات الجنائي.

ولابد لنا أن نوضح أن البينة الإلكترونية مسمى غير دقيق فإذا رجعنا إلى تعريف البينة نجدها هي ما يبين به الشيء من الدلالة الواضحة عقلية كانت أو محسوسة فالبينة ما يبين الدعوى ويظهر المقصود وهى حجة المدعى التي يثبت بها دعواه ولما كان الدليل الإلكتروني صادراً من أجهزة، إن جاز التعبير، وليس من حجة لفظية ينطق بها المدعى كان تسمية بينه إلكترونية تسمية غير موفقه لذلك فمن الاوفق ان نطلق عليها الدليل الإلكتروني.أما في الشريعة الإسلامية فذهب جمهور الفقهاء في أن البينة هي شهادة الشهود بينما ذهب (إبن تيمية،إبن القيم،وإبن فرحون وإبن حجر العسقلاني) إلى أن البينة هي:كل ما يبين الحق ويظهره من الشهود والإقرار والقرائن وغير ذلك. ولم اجد امثل من الادله الالكترونية فهى اوفق من البينة .

أما الدليل لغة :

جاء في مختار الصحاح أن الدليل هو مايستدل به والدليل الدال أيضا وقد (دله)على الطريق يدله بالضم ، و(دلاله) بفتح الدال وكسرها و(دلوله)بالضم والفتح أعلى ، ويقال (ادل) فأمل والاسم (الدالة) بتشديد اللام،وفلان (يدل) بفلان أى يثق.[3]

[3] مختار الصحاح ، باب الدال ، دلل ، مرجع سبق ذكره، ص 88.

أما الدليل شرعا:

فقد عرفه الإمام الشريف على بن محمد الجرجاني في كتاب التعريفات بأنه هو مايلزم من العلم به العلم بشيء أخر ،فإذا اعلم القاضي بحجته على دعواه ،لزم على من علم القاضي بتلك الحجة مع اقتناعه بها عامة بصدق دعوى المدعى فيما ادعاه ،والحكم له به.

أما الدليل اصطلاحا:

فقد وجدت أن التعريف الأمثل هو ما جاء به دكتور. فاضل زيدان إذ عرفه بأنه (الوسيلة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى الحقيقة من خلال تقديره السليم لها). [4]

وأجد نفسي متفقاً مع هذا التعريف لأن القاضي أثناء نظر الدعوى يقوم بتقييم أدلة القضية ويقوم بوزنها وتكييفها ويستقى منها قناعته في المرحلة النهائية ،والحاسمة عند الفصل في الدعوى فيحكم وفقاً للقناعة التي توصل إليها إما بالبراءة أو الإدانة وذلك حسب قوة الأدلة المطروحة أمامه.[5] ولا بد لنا هنا أن نميز ما بين الدليل وإجراءات الحصول عليه فوسيلة الحصول عليه لا تعتبر دليلا مثل الاستجواب والتفتيش والمعاينة ومراقبة الاتصالات الهاتفية فهذه الإجراءات لا تعد أدلة وإنما تعتبر مصدراً ينتج الدليل كذلك لابد لنا من التمييز بين الدليل والاستدلال وهى المرحلة التي تسبق الحصول على الدليل وهى المرحلة التحضيرية السابقة للحصول على الدليل فمثلا إجراءات التفتيش في مكان للحصول على دليل لا تُجرى ولا يؤُذن

[4] مختار الصحاح مرجع سابق ذكره ، 83.

[5] فاضل زيدان ، سلطة القاضى الجنائى فى تقدير الادله (ب ت)،(ب ن) ص 142

بها إلا بعد التحري من أجل الوصول إلى احتمال وجود فائدة مرجوة من التفتيش ولا بد لنا كذلك من التمييز بين الدليل والدلائل حيث أن الدلائل هي استنتاج واقعة مجهولة من أخرى معلومة وهذا الاستنتاج يكون على سبيل الاحتمال والترجيح. وضبط الاجهزة الالكترونية كما يعتقد البعض ليس دليلا على الاثبات وانما هى خطوة نحو الاثبات او تمهيدا للدخول الى الاثبات او النفى فالجرائم الالكترونية ليست مثل الجرائم التقليدية فحيازة المخدرات تشكل جريمة لذات المحاز اما حيازة الاجهزة ليست جريمة لذلك تحتاج الاجهزة العدلية فى كل الدول الى مزيد التدريب والتاهيل لمواكبة هذا العلم الجديد والمستحدث. ونجد أن الدلائل في الجرائم التقليدية مثل استعراف الكلاب البوليسية وتحريات الشرطة بإمكانها أن تكون معززه للأدلة الأخرى المتاحة في الدعوى بحيث تساعد في تكوين قناعة القاضي بالأدلة المتوفرة والتي عززت بالدلائل .

وعندما نتساءل عما إذا كانت كلمة دليل مرادفة لكلمة إثبات أم أن لكلا الكلمتين مدلول خاص بهما فقد درج الفقه على استخدام كلمة الإثبات للتعبير عن الدليل وكلمة الدليل للتعبير عن الإثبات وعلى الرغم من ذلك فإننا لا نجد تطابقاً بينهما فالإثبات يطلق على جميع المراحل التي تمر بها العملية ألإثباتيه والدليل يقدم مباشرة لبناء الحكم عليه .

تقسيمات الأدلة الجنائية:

تنقسم الأدلة الجنائية إلى عدة تقسيمات حسب وجهة النظر إليها سواء، من حيث مصدرها أو من حيث الجهة التي يقدم إليها الدليل أو من حيث علاقة الدليل بالواقعة المراد إثباتها. وكذلك من حيث الأثر المترتب عليها وأخيراً من حيث حداثتها،وسنتطرق إلى تلك التقسيمات.

من حيث المصدر:

تنقسم الأدلة من حيث المصدر إلى ثلاثة أقسام، أولها الأدلة المادية، وهي تلك الأدلة التي يكون مصدرها عناصر مادية، وتدل مباشرة على الواقعة المراد إثباتها، أي يمكن رؤيتها ولمسها ، كوجود الشيء المسروق في حيازة الجاني أو ضبط الجاني حاملاً سلاحاً استعمل في تنفيذ الجريمة أو آثار أقدام أو بصمات يعثر عليها في محل الحادث أو غيرها من الأمثلة، حيث أن الوسيلة التي ينتقل بواسطتها الدليل إلى علم القاضي، هي وسيلة، أو أداة مادية ملموسة،ويمكن الحصول على هذه الأدلة بوسائل متعددة كالكشف على محل الحادث والتفتيش والاستعانة بالخبراء.[6]

أما القسم الثاني : فهي الأدلة القولية أو الشفهية، وهي تلك الأدلة التي يكون مصدرها شخص معين، ويتمثل فيما يصدر عنه من أقوال،وتصل إلى علم القاضي ، وتؤثر في قناعة القاضي بشكل غير مباشر من خلال تأكده من صدق هذه الأقوال، وهذه الأدلة هي شهادة الشهود،سواءً كانوا شهود إثبات أم شهود نفي، واعترف المتهم بالتهمة المسندة إليه.

أما القسم الثالث: فهي الأدلة القانونية تلك الأدلة التي حددها المشرع سلفاً ، وعين قوة كل منها،بحيث لا يمكن الإثبات بغيرها، كما لا يمكن للقاضي أن يعطي أي دليل منها قوة أكثر مما أعطاها المشرع.

وهذا هو الأصل في المواد المدنية، أما في المسائل الجنائية ،فإن الأدلة غير محصورة في الغالب، والقاضي حرّ في تكوين عقيدته من أي دليل في الدعوى،ولكن في بعض الحالات يورد القانون قيوداً معينة على حرية القاضي في

---

[6] السيد محمد الحسن شريف ،النظرية العامة للاثبات الجنائي دراسة مقارنة (القاهرة : دار النهضة ، 2002م) ، ص 136

الاقتناع،فيحرم عليه الأخذ بدليل معين، أو يمنعه من الحكم بالإدانة، إلا إذا توفر دليل معين.

وفى تقديرى ان الادلة الالكترونية ادلة قاطعه وجازمه اذا ما تم الحصول عليها بصورة فنيه صحيحه فمثلا عنوان البريد الالكترونى هو عنوان لمستخدم واحد فى ساعة معينه ودقيقه وثانيه ومكان وعنوان هذا اذا كانت وسيلة الاتصال بالانترنت مسجلة تسجيلا صحيحا فهو يذهب بالاتهام الى شخص بعينه طبيعى او اعتبارى وعلى اقل تقدير يمكن محاكمته على المسئولية التقصيريه اذا ثبت عدم علمه بما تم ارتكابه من جرائم معلوماتيه عبر الانترنت او وسيلة الانترنت المسجله باسمه وهذا يمكن ان يستقر عليه القضاء سوابقا ويعمل على اثبات الجرائم المعلوماتية ،كما يمكن ان يدخل مزود خدمة الانترنت كمتهم اذا لم يكمل عملية تسجيل بيانات منفذ الانترنت بطريقه تمكنه من تقديم صاحب مرتكبى الجرائم بعناوينهم نسبة لدقتها كما اسلفنا.

ماهية الإثبات :

الإثبات بالكتابة:

الكتابة لغة هي الخط، وهو تصوير للألفاظ برموز كتابية، وفي الاصطلاح: [7]

هي الخط الذي يعتمد عليه في توثيق الحقوق وما يتعلق بها للرجوع إليها عند الإثبات، ويطلق عليها: الصك، والحجة، والسجل، وكتاب القاضي، والوثيقة، وتسمى في القانون: المستندات (جمع سند) والإثبات بالكتابة أهم وسيلة اليوم في القانون وأقواها وأكثرها استعمالاً، مع تقدم وسائل كشف التزوير، ومتى ثبتت الكتابة وجب الحق لصاحبه، واتفق العلماء على جواز الاعتماد على الخط والكتابة، لكن وقع

---

[7] انظر ابن منظور، لسان العرب، مادة ثبت 2/19-20؛ أبادي، القاموس المحيط، ص 190/ ص

الاختلاف في كتابات الأفراد بوصفها وسيلة مستقلة لإمكان التزوير فيها، وتشابه الخطوط والتوقيع، وصعوبة التطريق بين الصحيح والمزور، لأن الكتابة التي يعتمد عليها في الإثبات يجب أن تخلو من شائبة التزوير، ويجب التحقق من صحتها وسلامتها، ولذلك تطور الكشف عن تزوير الوثائق، واكتشاف التغيير حتى بأجهزة التصوير بالأشعة فوق البنفسجية، وصارت دراسة المستندات علماً يحتاج إلى مهارة وخبرة وتخصص دقيق.

تنقسم الكتابة فى الإثبات إلى ثلاثة أقسام : [8]

أ . المستندات الرسمية:

وهي التي يثبت فيها موظف عام أو شخص مكلف خدمة عامة، طبقاً للأوضاع القانونية، وفي حدود سلطاته واختصاصه، ما تمَّ على يده، أو تلقاه من ذوي الشأن. والمستندات الرسمية كلها حجة على الناس كافة فيما دُوّن بها، ولا تقبل إثبات العكس إلا بادعاء التزوير.

ب . المستندات العادية: التي تشتمل على توقيع من صدرت عنه، أو على خاتمه أو بصمة إصبعه، وليست لها صفة السند الرسمي.[9]

جـ . الأوراق غير الموقعة:

وتشمل دفاتر التجار، وتكون حجة ملزمة للقاضي فيما بين التجار، إذا كانت الدفاتر إجبارية ومنتظمة، وإلا كانت خاضعة لتقدير القاضي وقناعته بها، مع عدها حجة على صاحبها والثابت بالكتابة لا يجوز إثبات ما يخالفه إلا بالكتابة، ولو كانت قيمة

---

[8] أحمد فراج حسين، أدلة الإثبات في الفقه الإسلامي، ص 13، جرار كورنو معجم المصطلحات القانونية، 345/1.
[9] اشرف دوية – المجموعة الدولية للمحاماة – طعن رقم (2040) مجموعة المكتب الفني – مصر ج 42/1123

قليلة، كما تشترط بعض القوانين الإثبات بالكتابة حصراً في حالات، مثل عقد الشركة، وعقد الصلح، وعقد المقاولة وغير ذلك.

الإثبات بالشهادة:

الشهادة لغة: هي البيان والإظهار لما يُعلم، والمقصود بها في الإثبات إخبار عن ثبوت الحق للغير على الغير في مجلس القضاء والشهادة سبب لإحياء الحقوق، وحفظ الأرواح، وصيانة الأعراض. وكانت الشهادة في القديم أهم وسائل الإثبات لاعتمادها على الصدق والعقيدة، ثم أصابها الضعف والوهن لقلة الثقة بالناس، وانتشار الكذب وشهادة الزور، مع بقاء الاعتماد عليها اعتماداً رئيسياً في الوقائع المادية كالضرب والإتلاف، وفي الأحوال الشخصية. ويشترط في الشاهد أن يكون بالغاً عاقلاً، ناطقاً بصيراً، وأن لا يكون متهماً في شهادته بما يجرُّ بها نفعاً لنفسه، أو يدفع بها ضرراً أو مغرماً عنه، لذلك لا تقبل شهادة القريب، ولا الشهادة عند وجود خصومة أو عداوة بين الشاهد والمشهود عليه. لكن يشترط القانون أداء اليمين من الشاهد، ومنع القانون شهادة الأصل للفرع والعكس كالأب والابن، وشهادة أحد الزوجين للآخر، ويشترط أن توافق الشهادة الدعوى. ولم يحدد القانون نصاباً للشهادة، وأجاز شهادة الشاهد الواحد، واعتبرها حجة كاملة، وبينة تامة، وترك الأمر للقاضي في قبول الشهادة لتكوين القناعة منها، لأنَّ (المدارَ في الشهادة على الوزن لا على العدد) ويتعلق الأمر بوقائع الحال وضمير القاضي، لكن القانون اشترط إشهاد اثنين في توثيق العقود الرسمية.

أ- يجوز الإثبات بالشهادة استثناء عند تخلف الخصم عن الحضور للاستجواب، أو عند امتناعه عن الإجابة، فتكون هذه الحالة قرينة على ترجيح جانب الطرف الثاني، فتقبل منه الشهادة مهما كانت قيمة الالتزام.

ب- يجوز الإثبات بالشهادة استثناء عند وجود مانع من الحصول على دليل كتابي، سواء كان المانع أدبياً، كالالتزام بين الأقارب والمصاهرة.

ت- ويجوز الإثبات بالشهادة عند اتفاق الطرفين على التنازل عن الدليل الكتابي، وقبولهم الشهادة.

الإثبات بالإقرار:

الإقرار بينة وحجة باتفاق، وسيد الأدلة، ويؤخذ به، ويعمل بمقتضاه لانتفاء التهمة، لأن العاقل لا يقر على نفسه عادة كذباً، ولذلك نص عليه القانون .ومتى صدر الإقرار مستوفياً شروطه ظهر الحق المتنازع فيه، وألزم المُقِرَّ ما أقر به، ووجب على القاضي الحكم بموجبه، واعتبار الواقعة المقر بها صحيحة وأكيدة. لأن المرء مؤاخذ بإقراره، وإن الإقرار يبين الحق، ويظهر الواقعة، وتنتهي بعده الدعوى والخصومة بين الطرفين، ويؤمر المُقَرُّ بالتسليم ودفع المُقَرِّ به. والإقرار تثبت به جميع الحقوق، سواء أكانت في البدن، أم في المال، أم في الأحوال الشخصية، وسواء أكان فعلاً مشروعاً أم ذنباً وجريمة ومعصية ومخالفة، ويدخل في ذلك الإقرار بالنسب والوقف والوصية.

الإثبات باليمين :

هي (تأكيد ثبوت الحق أو نفيه باستشهاد الله تعالى أمام القاضي) واليمين وسيلة إثبات أمام القضاء باتفاق الشرائع والقوانين، لأنها تؤكد جانب الصدق ولها أثر كبير في المحاكم عند العجز عن تقديم الأدلة الأخرى.ولا تكون اليمين إلا بالله تعالى، لأن الحلف لتعظيم المحلوف به، ولا يجوز تعظيم شيء، أو التخويف منه، أو الزجر به، إلا بالله تعالى .ويشترط في اليمين أن يكون الحالف بالغاً، عاقلاً، مختاراً، وأن يكون المدعى عليه منكراً لحق المدعي، وأن يطلب الخصم اليمين من القاضي، فيوجهها القاضي إلى الحالف، وأن تكون اليمين شخصية تتصل بشخص الحالف مباشرة.

ويحدد طالب اليمين صيغتها بشرط أن تكون صريحة وظاهرة وغير قابلة للتأويل، ويحق للمحكمة تعديلها. واليمين في القانون إمّا غير قضائية، وهي التي تحلف، أو يتفق على حلفها في غير مجلس القضاء، وإمّا قضائية أمام القاضي.

ولليمين القانونية أنواع: حاسمة، ومتممة، واستظهارية

الإثبات بالقرائن :

والقرينة إمّا أن تكون قوية، وتعد دليلاً مستقلاً في الإثبات، وتسمى القرينة القاطعة، كالخلوة في استحقاق المهر، وإمّا أن تكون دليلاً مرجحاً لما معها، ومؤكدة له، كالوصف الصحيح من المؤجر والمستأجر في ملكية شيء في المأجور، وإمّا أن تكون دليلاً مرجوحاً، فلا تقوى على الاستدلال بها، وهي مجرد احتمال وشك فلا يعول عليها في الإثبات، وتستبعد في مجال القضاء، كوضع اليد على عين للدلالة على الملك، مع وجود دليل يثبت ملكية الغير.

الإثبات بعلم القاضي: المراد بعلم القاضي يقينه المؤكد الذي يُجوِّز له الشهادة مستنداً إليه مما عرض أمامه في المحكمة. ولا يجوز للقاضي أن يبني قناعته على ما يكون قد اطلع عليه شخصياً من وقائع خارج المحكمة، أو من غير أطراف النزاع.

الإثبات بالمعاينة: المعاينة أن يشاهد القاضي بنفسه أو بواسطة اخرين محل النزاع بين المتخاصمين لمعرفة حقيقة الأمر.[10]

الإثبات بالخبرة: والخبرة هي العلم بالشيء على حقيقته

---

[10] أحمد فراج حسين ، مرجع سبق ذكره ، ص 23.

محل الإثبات في المسائل الجنائيه: إن محل الإثبات في المسائل الجنائية هو الوقائع وحدها، وذلك بإقامة الدليل على وقوع جريمة بإثبات ركنيها المادي والمعنوي.

عبء الإثبات في المسائل الجنائية: تعتمد المسائل الجنائية على قاعدة فقهيه معروفه ، وهي أن الأصل في الإنسان البراءة، وكل متهم بريء حتى ينهض الدليل على إدانته . اما فى الجريمة الالكترونية يجب ان يكون شاهد الخبرة مجاوبا عن ما يدور داخل الجهاز المضبوط وان تقدم شهادتة امام المحاكم بناء على ماهو مثبت فى جهاز الكترونى مضبوط باجراء صحيح ومحفوظ وفق ما يوضح القانون وبالطريقة التى تحفظ بها الادلة والا فلا ،ولخصوصية الجرائم المعلوماتية فنجد انه ليس من الاوفق لقضاة محاكم الموضوع بناء احكامهم او عقيدتهم فى القضايا على تحرك شاهد الخبرة فى الشبكة المعلوماتية ومهارتة فى التعامل مع الحاسوب فليس فى ذلك دليل يدين المتهم الا مخرجات حاسوب ماثل امام المحكمة .

طرق الإثبات في المسائل الجنائية: لا يجوز استخدام وسيلة إثبات من شأنها المساس بالقيم الأساسية للحياة، كاللجوء إلى التعذيب، واستخدام ألوان القسوة أو العنف، ويجب الامتناع عن كل مساس بالسلامة الجسدية، والامتناع عن جميع الوسائل التي تنافي الأخلاق السليمة كالتنصت على الهاتف، والمذياع السري، والتسجيل الخفي، وأسلوب التحريض أو التوريط عن طريق العملاء المحرِّضين، والغالب معارضة استعمال الوسائل العلمية الحديثة كسبر غور المتهم، والتنويم المغنطيسي، واستعمال العقاقير، وآلة تسجيل النبض، لكن لا مانع من أخذ قطرات من دم المتهم والبصمات لفحصها وتحليلها. ويمكن تصنيف وسائل الإثبات الجنائية إلى ما يأتي:

أ- **المعاينات المادية:** كمكان الجريمة، والمواد المضبوطة التي تؤدي إلى كشف الجريمة بالطرق والوسائل التى حددها القانون.

ب- **شهادات الشهود:** وهم الشهود الذين شهدوا الواقعة ، مع تحليفهم اليمين القانونية، بعد دعوتهم رسمياً لذلك.

ت- **استجواب المدعى عليه:** وهذا الاستجواب قد يؤدي إلى الاعتراف، وهو أهم وسيلة في التحقيق. ويعد الاستجواب أيضاً وسيلة من وسائل الدفاع التي تمكّن المدعى عليه من بيان وجهة نظره بحرية تامة، من دون اللجوء إلى التعذيب والإيذاء والإرهاق والغش والخديعة والحيل. والاستجواب له فائدة محققة في جميع مراحله، لكن الأقوال التي يدلي بها المدعى عليه أمام رجال الشرطة، وأمام قاضي التحقيق تفقد قيمتها وسلطانها ومفعولها أمام قضاة المحكمة إلا إذا اعترف المدعى عليه من جديد أمام قاضي المحكمة بها.

القرائن: وهي وقائع مادية يمكن أن يستنتج من وجودها وجود الوقائع وبيان سير الأحداث، والاقتناع بوجود أركان الجريمة .

ويلجأ القضاء الجنائى باستمرار إلى القرائن والاستنتاجات منها، وخاصة لثبوت القصد الجنائي الذي يصعب استظهاره عملياً إلا بالقرائن والافتراضات العقلية وتتوقف قوة القرائن في الإثبات على كثرة عدد القرائن الصادقة التي تدل هذه القرائن عليها، وبعض القرائن لها تأثير قوي وفعال مثل البصمات والخبرة الفنية في الأسلحة والذخائر وتحديد القذائف، وكذا تحليل الآثار والبقع والأتربة.

الجرائم الالكترونية

يجدر بنا قبل أن نتعرض للجرائم المعلوماتية ان نقدم نبذة عن أصل اصطلاح المعلوماتية واصطلاح الرقمية :

فالمعلوماتية مشتقة من المعلومة او المعلومات وفنياً هنالك علاقة بين البيانات والمعلومات ،فالبيانات هي مجموعة من الحقائق او المشاهدات والقياسات

التي تكون عادة في شكل حروف او ارقام او اشكال خاصة توصف او تمثل فكرة او موضوعاً او هدفاً او شرطاً او اي عوامل أخرى وتمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات ،فالبيانات تعد مصطلحاً عاماً لكل الحقائق والارقام والرموز والحروف فهي معطيات اولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات[11]. ويتضح لنا من ذلك ان البيانات هي المادة الخام للمعلومات والتي لم يتم معالجتها بعد اما بعد معالجتها فأنها تتحول من بيانات الى معلومات.[12].

وتعرف المعلومات الالكترونية بأنها : ((كل مايمكن تخزينة ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والارقام والحروف والرموز والاشارات وغيرها)).

ولم يعرف المشرع السوداني صراحة المعلومات لكنه عرف الكتابة الالكترونية بأنها:((كل حروف او ارقام او رموز او اي علامات اخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو اي وسيلة اخرى مشابه وتعطى دلالة قابلة للإدراك)).

ماهية الجرائم المعلوماتية:

مصطلح الرقمية Digital

قد يعتقد البعض ان مصطلح الجريمة الرقمية او الدليل الرقمي يعني ان موضوعهما هو الارقام او ينصب على الارقام وهو مايجافي حقيقة هذا المصطلح فهذا المصطلح التقني يرجع اصله الى استخدام النظام الرقمي الثنائي (0,1) وهي

1- ايمن عبدالله فكري ، جرائم نظم معلومات دراسة مقارنة رسالة دكتوراه كلية الحقوق جامعة المنصور ،ص 22-25

2- فمثلاً اذاقلنا ان عدد الطلاب الحاضرين بالفصل الدراسي هو 22 طالبةً يعد بيان واذا قلنا بأن العدد الاجمالي للطلاب المسجل بالفصل 25 طالباً فان هذا ايضاً ماهو الا بيان .

الصيغة التي تسجل بها كل البيانات (اشكال وحروف ورموز وغيرها) داخل الحاسب الالى ، حيث يمثل (0) وضع الاغلاق.

والواحد (1) وضع التشغيل ويمثل الرقم (0) او الرقم واحد (1) مايعرف بالبيت

8 مايعرف بالبايت (1).Bits ويشكل عدد 8 بت Bit

تعريف الجريمة المعلوماتية أوالرقمية(الالكترونية)

تعددت التعريفات الخاصة بالجريمة الرقمية او المعلوماتية واختلفت الاتجاهات حول هذا الامر بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لها فهنالك تعريف فني عام لجريمة الحاسب الالي بأنها : نشاط اجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الفعل الاجرامي المقصود كما ان هنالك تعريفاً يفصل العناصر فمن الناحية القانونية يقضي تعدد استعمالات الحاسب الالي واختلاف عناصرها وعملياتها إيجاد تعريف لكل عنصر او عملية ويحدد اركان كل نشاط إجرامي.[13]

ووفقاً لتعريف منطمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982م والذي اوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي كل فعل او امتناع من شأنه الاعتداء على الامور المادية والمعنوية يكون ناتجاً بطريقة مباشرة عن تدخل تقنية المعلومات ، ويعرف البعض الاخر [14]

الجريمة الرقمية او المعلوماتية بأنها : مجموعة من الافعال غير المشروعة وينص المشرع على تجريمها والتي تتعلق بالمعالجة الالكترونية للمعلومات أو نقلها .

---

[13] عبدالفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية – دار الكتب القانونية المحلة الكبرى 2007 ص 386

[14] جوهر بنت عبدالعزيز ال سعود ، الجرائم الالكترونية ومكافحتها

كما تعرف بأنها : أي سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الالي ويؤدي تحقيق الى أغراض غير مشروعة ، وهي أي فعل يعاقب عليه القانون يتطلب ارتكابه الدراية بتكنولوجيا الحاسب الالكتروني .[15]

وتعرف الجريمة الالكترونية بأنها : فعل أو أفعال غير مشروعة تتم بواسطة النظم البرامجية او نظم المعالجة الالكترونية للحاسب الالى او الشبكات الحاسوبية او شبكة الانترنت وما على شاكلتها .

وعلى ذلك فتتنوع الجرائم المعلوماتية وتتعدد لدرجة يصعب حصرها ما بين التزوير والتزييف الرقمي او المعلوماتي وتدمير وإتلاف البرامج والبيانات والمعلومات والسطو على البيانات والمعلومات والاحتيال الرقمي والتجسس و...... إلخ .

تقسيم الجرائم المعلوماتية (الالكترونية) [16]

اولاً : تصنيف الجرائم تبعاً لنوع المعطيات ومحل الجريمة :

أ- الجرائم الماسة بقيمة معطيات الحاسوب .

ب- الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة .

ت- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات).

ثانيـاً : تصنيف الجرائم تبعاً لدور الحاسب الالي في الجريمة :

1- الجرائم التي تستهدف عناصر (السرية والسلامة ومورفولجية المعطيات والنظم) وتضم :-

أ- الدخول غير القانوني (غير المصرح به).

---

[15] منيرة بنت فهد الحمدان ،الحاسب اداة الدجريمة ووسيلة اكتشافها

[16] أحمد خليفة الملط الجرائم المعلوماتية – دراسة مقارنة – مرجع سابق -106

ب- الاعتراض غير القانوني .

ت- تدمير المعطيات .

ث- اعتراض النظم .

ج- إساءة استخدام الأجهزة .

2- الجرائم المرتبطة بالحاسب الالي وتضم :

أ- التزوير الرقمي أو المعلوماتي .

ب- الاحتيال الرقمي أو المعلوماتي .

3- الجرائم المرتبطة بالمحتوى أو المضمون ، وتضم الجرائم المتعلقة بالأفعال الاباحية واللاأخلاقية .

4- الجرائم المرتبطة بالإخلال بحق المؤلف وقرصنة البرمجيات .

ثالثـاً : تصنيف الجرائم تبعاً لمساسها بالأشخاص والاموال :

1- طائفة الجرائم التي تستهدف الاشخاص وتضم طائفتين رئيسيتين هما :

أ- الجرائم غير الجنسية التي تستهدف الاشخاص

Non–Sexual Crimes Against person's

وتشمل القتل بالحاسب الالي **Computer Murder**

ب- طائفة الجرائم الجنسية **Sexual Crimes**

2- طائفة جرائم الاموال – عدا السرقة – أو الملكية المتضمنة أنشطة الاختراق او الإتلاف.

3- جرائم الاحتيال والسرقة **Fraud And Theft Crimes**

4- جرائم التزوير **Forgery**

5- جرائم المقامرة والجرائم الأخرى ضد الأخلاق والأداب **Offenses gambling and other**

6- جرائم الحاسب الالي ضد الحكومة .

الحاسب أداء وهدف :

ويتبين لنا من العرض السابق مدى لزومية الحاسب الالي في الجرائم المعلوماتية ، فلا جريمة معلوماتية بدون جهاز حاسب بمكوناته المادية والبرامجية فالحاسب الالي إما أن يكون هدفاً للجريمة او أداة لها او بيئة لها واخيراً أداة للكشف عنها ومكافحتها ، ويمكن توضيح ذلك على النحو التالي :-

أ- الحاسب الالي هدفاً للجريمة وذلك كما في حالة الدخول غير المصرح به الى النظام او زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها . وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم .

ب- الحاسب الالي أداة الجريمة لارتكاب جرائم تقليدية .

ت- يكون الحاسب الالي بيئة الجريمة : وذلك كما في تخزين البرامج المقرصنة فية أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وانشطة الشبكات الاباحية ونحوها .

ث- دور الحاسب الالي في اكتشاف الجريمة : يستخدم الحاسب الالي على نطاق واسع في جميع مراحل الاثبات الجنائي بدءاً من مرحلة جمع الاستدلات وحتى تنفيذ الحكم مروراً بالاثبات العلمي الجنائي المتمثل بأعمال الخبرة العلمية حيث يلعب الحاسب الالى ذاته دوراً رئيساً في كشف جرائم الحاسب الالى وتتبع

فاعليها بل و إبطال أثر الهجمات التدميرية لمخترقي النظم وتحديداً هجمات الفيروسات و إنكار الخدمة وقرصنة البرمجيات .

المجرم المعلوماتي:

يتميز المجرم المعلوماتي عن المجرم التلقيدي بأنه مجرم على درجة عالية من التخصص والمهارة فى استخدام الحاسب الالى ، لكنه يستغل كل ذلك أستغلالا غير مشروع تبدأ من التلصص والمعاكسات والتطفل الى أبشع أنواع الجرائم وأخسها كالتجسس والقتل والارهاب ونشر البرامج الإباحية .

ويمكن أيضاً تصنيف (المجرم المعلوماتي) إلى عدة مجموعات .[17]

أ- المتخصصون في مجال الحاسب الالي وهم يحتلون المرتبة الأولى بين مجرمي المعلوماتية.

ب- الموظفين الساخطون أو الحاقدون على مؤسساتهم فيقومون بإتلاف أو تدمير أو تسريب المعلومات الخاصة بالمؤسسة .

ت- موظفوا المؤسسة الذين لهم بعض المشاكل معها تدفعهم للانتقام منها ورد إعتبارهم عن طريق الإضرار بالمؤسسة وإلحاق فادحة بها .

ث- أشخاص ذو ميول ودوافع سياسية معينة تدفعهم لأختراق نظم الحسابات الالية غير المصرح بالدخول فيها والتي تحتوى على معلومات وبيانات غاية في السرية ،تتعلق بالدفاع والامن ،ويمثل المساس بها مخاطر كارثية .

ج-القراصنة أو المخترقون وهم اشخاص يستغلون الحاسب الالي من اجل التسلية ولكن بشكل غير قانوني ويمكن تقسيمهم الى فئتين :-

الهاكرز Hackers : القراصنة الهواة.

---

[17] خالد ممدوح ، فن التحقيق الجنائي في الجرائم الالكترونية ، (القاهره : دار الفكر الجامعي ، 2009م) ص 94.

الكراكرز Crackers: وهم القراصنة المحترفون .

ويصنف مجرمو المعلوماتية الي ثلاثة طوائف :(المخترقين ، والمحترفين، و الحاقدين) مع التميز بين صغار السن والبالغين الذين يتجهون للعمل معاً لتكوين تنظيمات إجرامية شديدة الخطورة ودوافع ارتكاب جرائم الحاسوب إما السعى الى تحقيق الكسب المالى أو الانتقام من صاحب أو رئيس العمل والاضرار به أو لإثبات الذات وإظهار المهارات الشخصية المعلوماتية والتقنية والتغلب على واضعي برامج الحماية والتأمين .

خصائص الجرائم المعلوماتية (الالكترونية):

تتميز الجرائم المعلوماتية عن الجرائم التقليدية بالعديد من الخصائص :[18]

1-تتم الجرائم المعلوماتية في بيئة رقمية معلوماتية قوامها النظم البرامجية المعلوماتية الحاسوبية واجهزة ومعدات وادوات وتجهيزات الحاسب الالي ، اي تتم في وبواسطة جناحي الحاسب الالى :

- مكوناته المادية Hardware
- مكوناته البرمجيات Software

2-يقوم بها مجرم ذو طبيعة خاصة وامكانيات خاصة – علمية معلوماتية – يستخدم في ارتكاب جريمته الموارد المعرفية Knowledge Ware والاساليب الإحترافية .

3-صعوبة الحصول على دليل مادي يمثل هذه الجرائم حيث تغلب الطبيعة الالكترونية على الدليل المتوفر[19] .

[18] جميل عبد الباقي الصغير ، الحاسب الالي كوسيلة لأثبات الجرائم ، بحث مقدم لمركز دراسات الشرطة ، أكاديمية مبارك للأمن 2009م ص 84.
[19] . نبيل عبدالمعم جاد – أسس التحقيق والبحث الجنائي العلمي – ص 373

4-تستعصى على الاثبات بالطرق التقليدية وتستلزم طرقاً خاصه مستحدثة للإثبات ،قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسب الالى لذا فأنها تقتضي وجود رجل شرطة معلوماتي ومحقق معلوماتي وقاضي معلوماتي فضلاً عن الخبير المعلوماتي ، حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم لذا فأن عملية الاستعانة بالخبرة الفنية المتخصصة المؤهلة والمدربة تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي الذي يقدم للمحكمة لتقرير البراءة او الادانة فضلاً عن حتمية تدريب رجال الشرطة والنيابة والمحققين والقضاة على نظم وتكنولوجيا المعلومات وكيفية ضبط وتداول التعامل وفهم الادلة المختلفة عن هذة الجرائم .

5-هذه الجرائم لا تحدها حدود فهي جرائم عابرة لحدود المكان فيمكن عن طريقي الحاسب الالي – أو حتي هاتف نقال – لشخص في الصين ان يرتكب جريمة تزوير أو تزوير او تزييف أو سرقة معلومات أو نقود او ......إلخ ضد شخص طبيعي او معنوي في الولايات المتحدة الامريكية او العكس .

6-تتم في وقت ضئيل أحياناً لا يتعدى ثانية أو جزء من الثانية في بعض الجرائم .

7-تدنى نسبة الابلاغ عن تلك الجرائم من المجني عليهم – خاصة في حالة شركات ومؤسسات الاعمال لتجنب الإساءة للسمعة ورغبة في عدم زعزعة ثقة العملاء[20]،ففي إحدى الوقائع تعرض أحد البنوك هو بنك **Merchant bank** في بريطانيا لسرقة 8 مليون جنيه إسترليني من إحدى أرصدته الى رقم في سويسرا وتم ضبط الفاعل متلبساً بسحب المبلغ المسروق وبدلاً من محاكمته قام البنك بدفع مليون حنيه له بشرط التزام الفاعل بعدم الاعلام عن جريمته وإعلام البنك عن الالية التي نجح من خلالها في اختراق نظام الامن بحاسوب البنك الرئيسي.

[20]أحمد خليفة الملط الجرائم المعلوماتية – دراسة مقارنة – مرجع سابق -106

8-غالباُ ماتكون الخسائر الناجمة عنها فادحة للمجني عليه[21] .

9-مجموعة قراصنة أنونيموس التي شنت هجوماً عنيفاً يوم السبت الموافق 6 أبريل 2013م على الاف المواقع الاسرئيلية منها مواقع رئيس الوزراء ووزارة الدفاع وكانت خسارة اسرائيل من جراء ذلك الهجوم يتجاوز الثلاثة مليار دولار .

المبحـث الثانــي : جرائم الانترنت

تعتبر جرائم الانترنت هي النوع الشائع الان من الجرائم إذ انها تتمتع بالكثير من المميزات للمجرمين تدفعهم الي ارتكابها ويمكن تعريف تلك الجرائم بأنها ((الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بهما)).

خصائص جرائم الانترنت (CHARACTERISTICS OF INTERNET CRIMES)

وتعتبر الجرائم التي ترتكب من خلال شبكة الانترنت INTERNET CRIMES متفردة لا تتوافر في أي نوع من الجرائم CHARACTERISTICS وهي من الجرائم ذات الخصائص التقليدية في اسلوبها وطريقة ارتكابها والتي ترتكب يومياً في كافة دول العالم والتي لها انماط أخري مغايرة تماماً لخصائص تلك الجرائم التي ترتكب عبر الانترنت وتلك الخصائص الخاصة بجرائم الانترنت وهي :- [22]

1- في جميع الاحوال يكون الحاسب الآّلي هو أداة ارتكاب الجريمة.

2- ترتكب تلك الجرائم عبر شبكة الانترنت.

3- ان مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآّلى .

---

[21] نبيل عبدالمعم جاد – أسس التحقيق والبحث الجنائي العلمي – ص 373

[22] يونس خالد عرب (جرائم الحاسوب) دراسة مقارنة رسالة الماجستير 1994م ص 72

4- أن الجريمة لا حدود جغرافية لها .

الخصيصه الأولي :الحاسب الآّلي هو أداة ارتكاب جرائم الانترنت

خاصية الحاسب الآّلي هي دائماً أداة الجريمة في الجرائم التي ترتكب علي شبكة الانترنت هي خاصية متفردة عن أي جريمة أخري ذلك أن الحاسب الآّلي هو الاداة الوحيدة التي تمكن الشخص من الدخول علي شبكة الانترنت وقيامة بتنفيذ جريمته أيا كان نوعها وعليه فالحاسب الآّلي هو الاداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب علي شبكة الانترنت.

الخصيصه الثانية : الجرائم التى ترتكب عبر شبكة الانترنت

تعد شبكة الانترنت هي حلقة الوصل بين كافة الاهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الاهداف التي غالبا ماتكون الضحية لتلك الجرائم وهو ما دعا معظم تلك الاهداف الي اللجوء الي نظم الامن الالكتروني في محاولة منها لتحمي نفسها من تلك الجرائم أو علي الاقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم.

الخصيصه الثالثة : مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآّلي

لاستخدام الحاسب الآّلي لارتكاب جريمة علي شبكة الانترنت لابد و ان يكون مستخدم هذا الحاسب الالي علي دراية فائقة و ذو خبرة كبيرة في مجال استخدامه و إلا فمن أين له الخبرة اللازمة التي تمنكه من تنفيذ جريمته في العمل علي عدم اكتشافها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآّلي وان الشرطة تبحث أول ماتبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم .

الخصيصه الرابعة : الجريمة لا حدود جغرافية لها

شبكة الانترنت الغت اي حدود جعرافية فيما بين الدول وبعضها إذ يمكن التحدث فيما بين أشخاص ليس في بلدان مختلفة و إنما في قارات مختلفة في نفس الوقت علي شبكة الانترنت من خلال الدردشة وعليه فأن أي جرائم ترتكب عبر شبكة الانترنت فأنها تتخطى حدود الدولة التي ارتكبت فيها لتتعدى أثارها كافة البلدان علي مستوى العالم [23].

اهداف الجرائم الإلكترونية:

من المعروف ان اكثر الجرائم الالكترونية التي يتم ارتكابها يكون الهدف الاساسي لها هو الحصول علي المعلومات الالكترونية التي تكون اما محفوظة علي اجهزة الحاسبات الالية او تلك المنقولة عبر شبكة الانترنت وعليه فسوف نتعرض لأهداف الجرائم الالكترونية:-

1- المعلومات

هناك العديد من الجرائم التي يكون ارتكابها لهدف يتعلق بالمعلومات ويتمثل هذا الهدف أما بالحصول علي المعلومات أو تغييرها أو حذفها نهائياً وهذ الهدف تعرضنا له تحت عنوان أمن المعلومات معظم تلك الجرائم التي يكون الهدف منها المعلومات هي في الاغلب الأعم من الحالات تكون جرائم اقتصادية للحصول علي مزايا أو مكاسب اقتصادية فالحرب الاقتصادية لاتقل في ضراوتها وشدتها حالياً عن الحرب العسكرية ألا انها تتم عبر شبكة الانترنت .

---

[23] عبدالعال الديري – المركز العربي لابحاث الفضاء الالكتروني- بحث منشور في موقع المركز 2013/1/13

2-أجهزة الكمبيوتر

أما عندما يكون الهدف من ارتكاب الجرائم الالكترونية عبر شبكة الانترنت هو أجهزة الكمبيوتر فالغالب يكون الهدف هو تخريب تلك الاجهزة نهائياً أو على الأقل تعطيلها لأطول فترة ممكنة ومعظم تلك الجرائم تتم بواسطة استخدام الفيروسات.

3- الأشخاص أو الجهات

معظم الجرائم التي ترتكب عبر شبكة الانترنت تستهدف اما اشخاص او جهات بعينها وغالباً ماتكون تلك الجرائم هي جرائم مباشرة ترتكب في صورة ابتزاز أو تهديد أو تشهير أو جرائم غير مباشرة ترتكب في صورة الحصول علي البيانات والمعلومات الخاصة بتلك الجهات أو الاشخاص وذلك لاستخدام تلك المعلومات والبيانات بعد ذلك في ارتكاب جرائم مباشرة .

أضرار جرائم الانترنت:

وقد أجريت عدة دراسات عن جرائم الانترنت منها تلك الدراسة التي أجرتها منظمة (ALLIANCE BUSINESS SOFTWARE) وجرائم الحاسب الالي حيث تراوحت بين ثلاثين مليون دولار أمريكي في المملكة العربية السعودية والامارات العربية المتحدة ومليون واربعمائة الف دولار امريكي فقط في لبنان.[24]

[24] ويكيبيديا الموسوعة الحرة- الشبكة العنكبوتية

وقد أظهرت دراسة اخرى اجرتها هيئة الأمم المتحدة حول جرائم الانترنت أيضاً حوالي أربعون في المائة من منظمات القطاع العام والخاص علي السواء كانت ضحية لجرائم الانترنت والحاسب الآلي .[25]

وقد قدرت الولايات المتحدة الامريكية اضرار جرائم الانترنت والحاسب الآلي التي تكبدتها حوالي أن تكلفة جريمة الحاسب F.B.I خمسة مليارات دولار سنوياً كما قدرت المباحث الفيدرالية الامريكية الآلي أو الانترنت الواحدة حوالي ستمائة الف دولار سنوياً مقابل مبلغ ستة آلاف دولار تكلفة جرائم السرقة بالإكراه وبينت دراسة أخري أجراها أحد مكاتب المحاسبة الامريكية أن حوالي مائتين وأربعون شركة أمريكية قد تضررت من جرائم الغش باستخدام الكمبيوتر.

وأظهرت دراسة أخري أجريت من قبل منظمة عام 1999م أن خسائر حوالي مائة وثلاثة وستون شركة أمريكية من جرائم الحاسب الالي والانترنت قد بلغت اكثر من مائة وثلاثة وعشرون مليون دولار في حين أن الدراسة التي اجريت في عام 2000م قد أظهرت أن عدد الشركات التي تضررت قد زاد إلي ان اصبح مائتان وثلاثة وسبعون شركة تخطت خسائرها مبلغ مائتان وستة وخمسون مليون دولار .

إثبات جرائم الانترنت:

وجرائم الانترنت كثيرة ومتنوعة ويصعب كشفها وحصرها ومتابعة مرتكبها لان تلك الجرائم لا تترك أثرا يقود ألي مرتكبها .

تعود أسباب صعوبة أثبات جرائم الحاسب الالي والانترنت الي خمسة أمور كالأتي:- [26]

---

[25] ويكيبيديا الموسوعة الحرة – الشبكة العنكبوتية

[26] اضواء على الاثبات في الجرائم المعلوماتية – منتدى شئون قانونية – منتديات استارز تايمز

1-لا أثر للجريمة بعد ارتكابها .

2- صعوبة الاحتفاظ الفني باثارها أن وجدت .

3- أنها تحتاج الي خبرة فنية وتقنية ويصعب علي المحقق التقليدي التعامل معها

4- تعتمد علي الخداع في ارتكابها والتضليل في التعريف علي مرتكبيها.

5- تعتمد علي قمة الذكاء والمهارة في ارتكابها .

ومع تلك المصاعب الي تواجه اثبات جرائم الحاسب الالي والانترنت إلا إن الأمر ليس بهذه الصعوبة لذلك لابد من الأخذ بعدة خطوات ليكون في الإمكان مكافحة مثل تلك النوعية من الجرائم وفق الخطوات التالية :- [27]

1- تحديد الجريمة من البداية .

2- تحديد الجهة التي المنوط بها التعامل مع تلك الجرائم .

3- العمل علي تأهيل عناصر تلك الجهات ليكونوا على المستوي التقني الذي يمكنهم من العمل ومواجهة هذا النوع من الجرائم .

4- تعديل القوانين بمايتناسب مع تلك الجرائم التي استجدت على وضع العقاب الشديد لها لتكون مانعاً من موانع ارتكاب مثل تلك الجرائم بصفة دولية بإقرار اتفاقية دولية تجرم تلك الجرائم .

5- التركيز على مواجهة تلك الجرائم وتعمل كل الدول علي ملاحقة مرتكبيها.

فوائد شبكة الانترنت:

---

[27] حسين الغافري ، ومحمد الالفي ، جرائم الانترنت بين الشريعة الاسلامية والقانون، دار النهضة العربية ، 2008م ص 72

الانترنت ليست مرتعاً لارتكاب الجرائم وانما هي أيضاً تقدم خدمات جليلة للأمن احياناً منها :-

1- تتسم بالسرعة والفورية متجاوزة للمعيار الزمنى والجغرافي.

2- إضفاء نطاق من السرية فيما بين الأمن والمتعاونين معهم بمعني عدم تعريض المتعاونين مع الامن للخطر.

3- إعطاء الفرصة لمن لديه معلومات من الجمهور أن يقدمها للأمن بطريقة سرية دون تعريض حياته للخطر.

4- يساعد الامن في توسيع إطار البحث عن المجرمين بنشر صورهم وطلب الإبلاغ عن أي معلومات عنهم على الشبكة ليطلع عليها اكبر عدد ممكن من الاشخاص لتضييق الخناق و القبض عليهم.

5- وسيلة لنشر أي معلومات أو بيانات أو قوانين أو قرارات جديدة تهم المواطنين واستقبال معلومات المواطنين بسهولة .

6- من خلال شبكة الانترنت وما عليها من مواقع يمكن توفير فرص العمل للشباب.

7- يمكن ان يتم استخدام المواقع علي شبكة الانترنت في عمل الاستفتاءات على جميع القضايا سواء الوطنية أو العالمية ومن خلال تلك الاستفتاءات يتم قياس مستوى رأى الجمهور فيما يعرض علي القيادة السياسية من قضايا وطنية .

8- تعتبر الشبكة وسيطاً فاعلاً في عملية تدريب العاملين بمختلف المصانع والشركات وتعريفهم بأحدث أساليب العمل في المصانع والشركات المشابهة في الدول المتقدمة .

طرق إرتكاب جرائم الحاسب الآلي والانترنت :

يمكن تقسيم تلك الجرائم التي ترتكب عبر شبكة الانترنت إلي أنواع بحسب ما تستهدفه من الجريمة والطريقة في بلوغ هذا الهدف فعلى ذلك يمكن تقسيمها إلي أربع انواع :-

النوع الاول :-

وهى الجرائم التي تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآّلي لاستغلالها بطريقة غير مشروعة ويتميز هذا النوع من الجرائم بصعوبة اكتشافه .

النوع الثانــي :-

وهذا النوع من الجرائم يستهدف مراكز معالجة البيانات المخزنة في الحاسب الالي بقصد التلاعب بها أو تدميرها كلياً أو جزئياً ويمثل هذا النوع الفيروسات المرسلة عبر احد الوسائط المتنوعة مثل البريد الالكتروني E-MAIL .

النوع الثالث :-

وهو استخدام الحاسب الالي في ارتكاب الجريمة وقد وقعت جريمة من هذا النوع في إحدى الشركات الامريكية التي تعمل سحباً علي جوائز يانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الالي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة لشخص بطريقه غير مشروعة .

النوع الرابـع :-

ويشمل إساءة استخدام الحاسب الالي أو استخدامه بشكل غير قانوني من قبل الاشخاص المرخص لهم باستخدامه ومثال ذلك استخدام الموظف الحاسب الالي في امور خاصة لا تختص بالعمل بعد إنتهاء وقت العمل .

المبحث الثالـث : مكافحة جرائم الانترنت

مكافحة الجرائم الالكترونية:

1- التعاون الدولي في المكافحة:

للتعايش السلمي بين الدول لابد من الامان والاستقرار ومن الوقع العلمى اتضح ان اي دولة لا تستطيع بمجهودها منفردة القضاء على الجريمة وسط هذا التطور المذهل في الاتصالات وتكنولوجيا المعلومات لذلك اصبحت الحاجة ماسة الي وجود كيان دولى يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله الدول المختلفة خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنه .

وهناك جهود الانتربول (الشرطه الجنائية الدولية) حيث:[28]

أ- تهدف هذه المنظمة الي تأكيد التعاون بين أجهزة الشركة في الدول الاعضاء على نحو فعال في مكافحة الجريمة .

ب- وهناك ايضاً تبادل المعاونه لمواجهة المواقف الحرجة فضلاً عن القيام ببعض العمليات الامنية المشتركة.

ت- المساعدة القضائية الدولية وتعرف المساعدة القضائية الدولية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم وتتخذ المساعدة القضائية في المجال الجنائي عدة صور منها تبادل المعلومات ،ونقل الاجراءات وفق إتفاقية أو معاهدة ،الانابه القضايئة الدولية ، مع اعتبار فقه القانون الدولي تسليم المجرمين شكلاً من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين، وأخيراً التعاون الدولي في مجال التدريب على مواجهة الجرائم الالكترونية .

أن مكافحة الجرائم الالكترونية لن يكون له تأثير يذكر إلا إذا كان هناك تعاوناً دولياً علي اكبر قدر من التنسيق وعليه يمكننا القول أن أي مجهود أو اجراءات قد تقوم بها

---

[28] سراج الدين محمد الروبي ، ألية الانتربول في التعاون الشرطي ، القاهره : الدار المصرية اللبنانية ، 1998م ص 87.

أي من الدول علي مستوي العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم فتلك الجرائم لها طابع خاص تتسم به هو انها جرائم عابرة للحدود فهي لا تتم من داخل دولة ويكون تأثيرها منحصر في تلك الدولة وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دول أخرى وتكون أثارها ممتدة لتصل إلي عدد غير محدود من الدول وعليه فأن الاساس الذي يرتكزعليه مجال مكافحة الجرائم الالكترونية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج الضاره علي الكيانات الاقتصادية للدول.

وعليه فسوف يكون تناولنا لمكافحة الجرائم الالكترونية من خلال التركيز علي التعاون الدولي والعناصر التي يرتكز عليها هذا التعاون والتي تنحصر في الأتـي :- [29]

1- المعاهدات والمؤتمرات الدولية.
2- إصدار قوانين جديدة تجرم الجرائم الالكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق.
3- التعاون الدولي.
4- اتحاد الشركات والكيانات الاقتصادية الكبرى في مجال حماية أمنها الالكتروني.
5- المعاهدات والقوانين الخاصة بحق الملكية الفردية .

1- المعاهدات والمؤتمرات الدولية:

[29] عمر الفاروق الحسيني ، المشكلات الهامه في الجرائم المتصل بالحاسوب وابعادها الدولية ، دراسة تحليلية نقدية ،ط2 القاهرة 1995م ص 133.

تعد المعاهدات الدولية هي أساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الالكترونية وقد تم عقد العديد من المعاهدات التي تعمل علي التعاون الدولي في مجال مكافحة الجرائم الالكترونية ومن تلك المعاهدات :

أ- معاهدة بودابست لمكافحة جرائم الانترنت:

شهدت العاصمة المجرية بودابست في اواخر عام 2001م ميلاد أولى المعاهدات الدولية التي تكافح جرائم الانترنت تبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم الي حد خطير أصبح يهدد الاشخاص والممتلكات.

ويعد التوقيع علي تلك المعاهدة الدولية – التي تهدف الي توحيد الجهود الدولية في مجال جرائم الانترنت التي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الاغلب الأعم من الحالات ودون أي غرض اجرامي الي مرحلة جديدة يقوم بها محترفون علي اعلي درجة من التخصص وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات الكثيرين من رواد شبكة الانترنت للخطر ،وهو الخطوة الاولي في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم علي شبكة الانترنت واستخدامها الاستخدام الاسوأ ، وقد صاغ نصها عدد من الخبراء القانونيين في مجلس أروبا بمساعدة دول أخرى وبالأخص الولايات المتحدة .[30]

وتحدد الاتفاقية أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها كما تحاول إقامة توازن بين

---

[30] معاهدة بودابست لمكافحة جرائم الانترنت 2001- المجر

الاقتراحات التي تقدمت بها اجهزة الشرطة والقلق الذي عبرت عنه المنظمات المدافعة عن حقوق الانسان والصناعات المعنية ومزودي خدمات الانترنت.

وتخشى منظمات حقوق الانسان من أن تحد الاتفاقية من حرية الافراد في أعقاب الهجمات على الولايات المتحدة، كما أن القلق يتزايد من أن تؤدي زيادة الرقابة إلي انتهاك حقوق مستخدمي الانترنت وهو يتعارض مع الاعلان العالمي لحقوق الانسان الصادر من الأمم المتحدة والذي ينص في المادة الثانية عشر منه على انه لايتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته كما أن المادة التاسعة عشر من هذا الاعلان تنص على انه لكل شخص الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الاراء دون أي تدخل واستقاء الأنباء والافكار ونقلها و إذاعتها بأي وسيلة كانت دون تقيد بالحدود الجغرافية .

إلا ان تلك الحقوق التي نص عليها الاعلان العالمى لحقوق الانسان الصادر من هيئة الأمم المتحدة لم يترك تلك الحقوق الانسانية لتمارس دون أي قيود إذ انه قد نص في المادة التاسعة والعشرون على انه يخضع الفرد في ممارسة حقوقه وحرياته إلي تلك القيود التي يقررها القانون فقط لضمان الاعتراف بحقوق الغير وحرياته واحترامها لتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والاخلاق في مجتمع ديمقراطي.

وعليه فنحن نرى أن تلك المعاهدة التي لا غرض لها إلا احترام حقوق الانسان والحد من تعرضه للكم الهائل من الجرائم التي ترتكب عبر شبكة الانترنت لا تتعارض بأي حال من الاحوال مع الاعلان العالمي لحقوق الانسان الذي يعد الأساس في تقرير حريات الأشخاص .

ت- المعاهدة الأوربية لمكافحة جرائم الإنترنت:

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الاوروبي علي المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الانترنت وسط انتقادات من دعاة حماية الحرية الشخصية وبعد أن تم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الاتفاقية الدول الموقعة عليها بسن الحد الادنى من القوانين الضرورية للتعامل مع الجرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلي شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

وتتضمن بنود المعاهدة التي تم تعديل مسودتها 27 مرة قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها في جمع الادلة وفرض القانون لكن الصلاحيات الدولية الجديدة ستكون علي حساب حماية المواطنين من إساءة الحكومات أستخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يسيئون استخدامها.

1- إصدار قوانين جديدة تجرم الجرائم الالكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق:

اتجهت كافة الدول المتقدمة تكنولوجيا إلي استخدام نصوص قانونية جديدة تجرم تلك الجرائم الالكترونية الجديدة علي قوانينها التقليدية القديمة وعليه فقد صاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجيا.

تعتبر دولة السويد من أوائل الدول االتي اتجهت إلي سن تشريعات قانونية جديدة خاصة بجرائم الانترنت والحاسب الالي لتستطيع أن تعاقب المتهمين بأرتكاب تلك الجرائم الالكترونية ، حيث صدر أول قانون خاص بها سمي بقانون (البيانات) وقد أصدر هذا القانون عام 1973م وقد عالج هذا القانون قضايا الاحتيال عن طريق

الانترنت بالإضافة الي كونه يشتمل على فقرات عامة من نصوصه لتشمل جرائم الدخول غيرالمشروع علي البيانات الالكترونية أو تزوير المعلومات الالكترونية أو تحويلها أو الحصول غير المشروع عليها .

وكانت الولايات المتحدة الامريكية هي الدولة التالية التي تبعت السويد في إصدار قوانين خاصة بها تجرم الجرائم الالكترونية حيث شرعت قانوناً خاصاً بحماية أنظمة الحاسب الألـي (1976م – 1985م) وفي عام 1985م حدد معهد العدالة القومي الامريكي خمسة أنواع رئيسية للجرائم المعلوماتية وهي :-[31]

1- جرائم الحاسب الألـي الداخلية

2- جرائم الاستخدام غير المشروع عن بعد

3- جرائم التلاعب بالحاسب الألـي

4- دعم التعاملات الإجرامية .

5- سرقة البرامج الجاهزة والمكونات المادية للحاسب .

في عام 1986م صدر قانوناً أخر يحمل الرقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون علي الجرائم المعلوماتية كما وضعت المتطلبات الضرورية اللازمة لتطبيقة ، وعلى أثر ذلك قامت الولايات الداخلية بإصدار التشريعات بكل منها على حده للتعامل بها مع تلك الجرائم الإلكترونية ومن تلك القونين القانون الخاص بولاية تكساس لجرائم الحاسب الألـي.

---

[31] هشام محمد فريد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني ، بحث مقدم الي مؤتمر القانون والكمبيوتر والانترنت في مايو 2002م

قد خولت وزارة العدل الامريكية في عام 2000م خمس جهات حكومية للتعامل مع جرائم الانترنت والحاسب الألي منها مكتب التحقيقات الفيدرالي .

أما بريطانيا فهي ثالث دولة تسن قانون خاص بها بجرائم الانترنت حيث أقرت قانون لمكافحة التزوير والتزييف عام 1981م الذي شمل في تعاريفه الخاصة تعريف أداة التزوير و وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخري يتم التسجيل عليها سواء بالطرق الالكترونية أو التقليدية أو أي طرق أخري .

أما كندا فهي تطبق قوانين متخصصة ومفصلة للتعامل مع جرائم الانترنت حيث عدلت في عام 1985م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الالي والانترنت كما شمل القانون الجديد أيضاًتحديد للعقوبات المطبقة علي المخالفات الحاسوبية وجرائم التدمير وجرائم الدخول غير المشروع علي المعلومات الالكترونية .

أما الدانمارك فقد انتبهت لهذا الامر مبكراً أيضاً فقد سنت أول قانون خاص بها في مجال مكافحة الانترنت والحاسب الالي في عام 1985م وقد شمل القانون العقوبات المحددة علي مايرتكب من جرائم مثل الدخول غير المشروع علي الحاسب الالي او تزوير البيانات سواء كان هذا التزوير بالحذف او الاضافة او التعديل.

أما فرنسا فهي الدولة التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة – جرائم الانترنت .

فقد طورت فرنسا قوانينها الجنائية لتتوافق مع المستجدات الاجرامية حيث اصدرت اول قانون خاص بها وفي عام 1988م القانون رقم (19-88) والذي اضاف الي قانون العقوبات الجنائي جرائم الحاسب الالي والعقوبات المقررة لتلك الجرائم كما تم في عام 1994م تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد

القانونية الخاصة بالجرائم المعلوماتية وقد أوكل هذا القانون الي النيابة العامة سلطة التحقيق فيها بما في ذلك طلب عمل التحريات وسماع الاقوال والشهود .

أما هولندا فقد قامت هي الأخري بتعديل القوانين الخاصة بها للتوائم مع تلك الجرائم الحديثة ليكون في امكانها التعامل معها ومحاولة السيطرة عليها فقد قامت بتعديل القوانين الخاصة بها ونصت في تلكم القوانين علي انه من حق القاضي أن يصدر أوامره بالتنصت علي شبكات الحاسب الالي متي ما كانت هناك جريمة خطيرة ومتي كان هذا التصنت علي قدر عال من الاهمية للكشف علي تلك الجريمة .

أما في دولة بولندا فهي ايضاً سنت القوانين الخاصة بها وتلك القوانين التي سنتها تنص علي ان للمتهم بارتكاب الجرائم الحق في عدم طبع أي سجلات خاصة بالحاسب الالي أو إفشاء كلمات السر المستخدمة أو حتي الاكواد الخاصة بالبرنامج كما انها تنص علي حقوق اخري بالنسبة للشهود في تلك الجرائم فهي تعطي الشاهد الحق في الامتناع عن طبع المعلومات المسترجعة عن الحاسب الالي متي كان ذلك قد يؤدي الي ادانته أو ادنة اي من اقاربه بل ان تلك القوانين تذهب الي مدى ابعد من ذاك فتلك القوانين تنص على ان لا يقابل ذلك أي اجراء قسري قد يتخذ وتكون من نتائجه إدانة بالمتهم .

أما عن الحال في الدول العربية فأنه للأسف لا يوجد أي دولة عربية قد قامت بسن قوانين جديدة خاصة بها أو حتي تحديث قوانينها الخاصة لتستوعب تلك المستجدات الاجرامية فالدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطوير الاجرامي بينما نجد ان الدول العربية لا زالت لا تحرك ساكناً.

فمصر علي سبيل المثال لا الحصر لم تعمل على سن قوانين جديدة خاصة بهافي هذا المجال ولم تقم حتي بتعديل مالديها من قوانين وانما القانونيين في مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي علي الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الافعال المشابهه بالافعال المكونة لاركان الجريمة المعلوماتية ومن ذلك علي سبيل المثال اعتبر ان قانون براءات الاختراع ينطبق علي الجانب المادي من نظام المعالجة الالية للمعلومات كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الاسراربحيث يمكن تطبيقها على بعض جرائم الانترنت و أوكل الي القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية .

وعليه فأن وجد نص قانوني يعاقب علي جريمة شبيهه بالجريمة المعلوماتية يتم ادراجها تحته وتقرر العقوبة المنصوص عليها في ذلك النص وعليه ودائماً وفي جميع الاحوال لا تكون العقوبة المنصوص عليها في ذلك النص القانوني تتناسب وحجم الخسائر الناتجة علي ارتكاب مثل تلك الجريمة الالكترونية ولانه لايوجد نص صريح خاص بها ويعاقب عليها ويعطي العقوبة المناسبة للاضرار الناتجة من تلك الجريمة يتم ادراج تلك الجريمة المعلوماتية تحت هذا النص القانوني غير الخاص بها والموضوع للعقاب على جريمة أخري وبالتالي لا يكون العقاب المنصوص عليه مناسب .

أما في المملكة العربية السعودية فهي لا تواجه نفس تلك المشاكل علي اساس أن كافة تشريعاتها تنطلق من الشريعة الاسلامية وبالتالي فهي لا تحتاج الي تحديث فالشريعة الاسلامية لا تحتاج الي اي تحديث فالشريعة الاسلامية صالحة لكل زمان ومكان .

وقد اتخذت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الانترنت المشرفة علي عمل مقدمي خدمة الانترنت في المملكة عدد من الاجراءات الفنية التي تهدف الي محاصرة اعمال المخربين والمتسللين ومنعهم وقد اوضحت الوحدة انها قد الزمت جميع مقدمي الانترنت في المملكة بتطبيق عدد من الاجراءات الفنية لمنع اعمال المتسللين وإساءة استخدام البريد الالكتروني وغيرها من المخالفات المتعلقة بالجوانب الامنية لاستخدام شبكة الانترنت في المملكة ومن بين هذه الاجراءات مايأتي :-[32]

1- منح انتقال أرقام الانترنت او مايعرف بخلالها بعض المتسللين المحترفين باستخدام ارقام بعض الاشخاص بطريقة غير مشروعة .
2- العمل علي منع إساءة البريد الإلكتروني أو سوء التهديد أو ارسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ماعرف اصطلاحاً بالبريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة ، اي الاحتفاظ بسجل استخدام مزود الاتصال الخاص DIALUP – SERVER لمدة لاتقل عن ستة أشهر.
3- الاحتفاظ بسجل استخدام البروكسي PROXY
4- الحصول علي خدمة الوقت عن طريق وحدة البروكسي ومزود الاتصالLTP بهدف اللجوء اليها لمعرفة توقيت حدوث عملية الاختراق للاجهزة أو الشبكات.
5- تحديث سجلات منظمة رايب الخاصة بمقدمي الخدمة .
6- ضرورة تنفيذ ماتتوصل اليه اللجنة الامنية الدائمة بخصوص متابعة ومعاقبة المخالفات الامنية .

من المعروف أن جرائم الانترنت هي جرائم عابرة للحدود أي أنها لا تتم وتنتهي في اراضي دولة بعينها وعليه فالتعاون ألدولى هو من أهم سبل مكافحة جرائم

[32] حسين الغافري ، ومحمد الالفي ، مرجع سبق ذكره ، ص 103.

الانترنت وملاحقة مرتكبيها فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة الي اخرى تبيح القوانين السارية بها ما ارتكبوه من جرائم .

وتعتبر المعاهدات الدولية التي تنضم اليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي في ذلك المجال. ومثال ذلك أيضا التعاون الدولي في مجال مكافحة الجريمة المنظمة وقد بدا هذا التعاون الدولي بمؤتمر الأمم المتحدة السابع والذي عقد عام 1985م لمنع الجريمة المنظمة حيث أعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة والقضاء عليها.

وكانت معاهدة المجلس الاوروبي حول جرائم الشبكات الالكترونية التي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعملية وضع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها في نهاية الامر في وجودها التشريعية والتنظيمية وتطبيق القوانين .

ويستند نهج هذة المعاهدة الى اعتراف اساسي بضرورة قيام انسجام بين قوانين الدول المعنية وقد تم تحقيق التعاون الدولي في تطبيق القوانين من خلال سلسلة من المعاهدات التي تمكن الحكومات من تبادل تسليم المجرمين والمساعدة القانونية المتبادلة للمعلومات والادلة وبغية وضع هذه المعاهدات قيد التنفيذ يفترض عادة وجود مايعرف بازدواج العمل الاجرامي (أي ان تكون السلطات القضائية لكلاً الدولتين تعتبر ذلك العمل عملاً جرمياً) وعليه يتم تسهيل التعاون الدولي بدرجة كبيرة من خلال التلاقي علي ما يمكن اعتباره عملاً إجرامياً بموجب تشريعات مختلف البلدان المعنية فأن فرض قوانين مماثلة في مختلف الدول يزيد المخاطر التي تواجه مرتكبي جرائم الانترنت ويتجه اكثر نحو معادلة هذه المخاطر في مختلف الدول المعنية وفي الواقع

كلما كانت القوانين أكثر شمولاً كلما قلت الملاذات الامنة التي يستطيع المعتدون على الشبكات الالكترونية العمل انطلاقاً منها بأمان .

ان الانسجام ضروري بالنسبة الي القوانين الاساسية كما بالنسبة الي القانونين الاجرائية وعلي كافة الدول ان تعيد تقييم ومراجعة قواعد الاثبات والتفتيش وإلقاء القبض والتصنت الالكتروني وما شابه ذلك لتشمل المعلومات الرقمية وأنظمة الكمبيوتر الحديثة وأنظمة الاتصالات الحديثة والطبيعية العالمية لشبكة الانترنت أما التنسيق الاكبر للقوانين الاجرائية فيمكن ان يسهل التعاون في التحقيقات التي تشمل سلطات قطاعية متعددة .

وعلى مستوي العالم العربي وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل في مكافحة الإرهاب والتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة وفي عام 1996م وافق المجلس في دورته الثالثة عشر على مدونة سلوك طواعية لمكافحة الإرهاب و وافق عام 1997م في دورته الرابعة عشر على استراتيجية عربية لمكافحة إلارهاب وفى عام 1998م أقر مجلس وزراء الداخلية والعدل العرب الاتفاقية العربية لمكافحة الارهاب هذا في مكافحة الجرائم المنظمة أما في مجال التعاون الدولي لمكافحة الاتجار في المخدرات فقد اهتمت كافة الدول بهذا الموضوع لما يسببه من أضرار علي اقتصادياتها وكذلك لما يسببه من إنهاك لثروتها البشرية والتي تعتمد عليها أي دوله في تحقيق تقدمها الاقتصادي وعليه فقد كان تعاوناً دولياً في مجال مكافحة الاتجار في المخدرات ومساعدة المدمنين على الإقلاع عن الإدمان .

وقد عقدت اتفاقية مكافحة المخدرات عام 1961م واتفاقية المؤثرات العقلية عام 1971م واتفاقية الأمم المتحدة لمكافحة الاتجار في المخدرات والمؤثرات العقلية عام 1988م .

وعلى المستوي العربي تم عام 1996م إقرار الاتفاقية العربية لمكافحة الإتجار في المخدرات والمؤثرات العقلية كما تم في عام 1996م إقرار القانون العربي النموذجي الموحد للمخدرات .

وعليه فإنه لتفيل التعاون الدولي لابد من التركيز على ثلاث موضوعات رئيسية لابد على العمل لتعظيم وجودها والأخذ بها وهى كالأتي :-[33]

أ- الانضمام الي المعاهدات الدولية التي تعمل علي زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مجال مكافحة جرائم الانترنت .

ب- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي أي تنفيذ ماتنص عليه تلك الاتفاقيات من إجراءات دون أي إبطاء .

ت- العمل على وجود أكبر قدر ممكن من التناسق والتطابق فيما بين قوانين الدول المختلفة والمتعلقة بجرائم الانترنت فلا يكون الفعل الذي تم ارتكابه جريمة في بلد ما وغير معاقب عليه في قانون بلد أخر فمن هنا يجد المجرمون الملاذ الأمن الذي يلجئون إليه دون أي اعتبار لما ارتكبوه من جرائم ، تعاون جميع الدول في تسليم المطلوبين أمنياًالى الدول التي تطالب بهم لارتكابهم جرائم الانترنت .

اتحاد الشركات والكيانات الاقتصادية في مجال حماية أمنها الالكتروني:

تعد الكيانات الاقتصادية من أهم الاهداف المحتملة لأي عمليات إجرامية تتم عبر الانترنت وغالباً مايكون الهدف من ارتكاب تلك الجرائم هو البحث عن أموال تلك الشركات الضخمة او عما تخفيه من معلومات تريد الشركات الاخرى الحصول عليها في محاولة منها في التغلب على ما تعانيه من نقص في المعلومات التكنولوجية التي تساعدها على النهوض تكنولوجيا وتصبح في عداد الشركات الاقتصادية الكبرى

---

[33] عكاشة محمد عبد العال ، الانابه القضائية في نطاق العلاقات الخاصة الدولية ،(بيروت : الدار الجامعية ، 1992م) ص 65.

والمتقدمة اقتصادياً بما يعود عليها من فوائد اقتصادية ضخمة وعليه فغالباً ما تكون الشركات الاقتصادية هي الهدف السمين الذي يلهث وراءه مرتكبي جرائم الانترنت.

أيضاً قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة هي الحصول على معلومات هامة عنها للقيام بابتزازها والحصول منها على مبالغ مالية في مقابل عدم نشر ماتم الاستيلاء عليه من معلومات في الغالب يكون نشرها ضارا بالشركة ضرراً بالغاً.

وعليه فأن الكثير من الكيانات الاقتصادية الهامة في العالم تتحد مع بعضها البعض في محاولة منها للقيام ببناء حائط صد الكتروني مضاد لما قد تتعرض له من هجمات ومحاولات اختراق وقرصنه من محترفي ارتكاب جرائم الانترنت ومكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها البعض في هذا الأمر .

1- فمن ناحية فأن التعاون الذي يتم بينها وبين الكيانات الاقتصادية الأخري يوفر قدراً كبيراً من الاموال فيما كانت ستقوم ببناء هذا الحائط المضاد بمفردها فعندها كانت ستتحمل بمفردها مايتكلفه من اموال دون أي مساعدة من أي جهة خارجية .

2- ومن ناحية اخري فأن هذا الاتحاد يكون ائتلافاً قوياً في مواجهة تلك الهجمات التتارية على تلك الكيانات وبالتالي يجعلها أقوي عند مواجهة تلك الاختراقات وصدها وتعقب مرتكبيها.

3- أن تعاون تلك الشركات وعدم تحمل أي منها للتكاليف بمفردها يجعلها تستطيع القيام ببناء حائط صد قوى ومنيع في مواجهة مرتكبي جرائم الانترنت وبالتالي يصعب من فرص اختراقه والنفاذ الى تلك الشركات .

وعليه نجد ان تعاون الكيانات الاقتصادية الكبرى في مجال مكافحة جرائم الانترنت يساعد كثيراً على حماية أمنها من مخاطر التعرض لتلك الجرائم ويحافظ عليها من اي

محاولات ابتزاز قد تتعرض لها إذا ما استطاع أي شخص النفاذ الى معلوماتها والحصول عليها فعندئذ سيكون عليها أن تدفع له الكثير من الاموال لمنعه من نشر معلوماتها السرية والتي قد تستفيد منها أي شركات منافسة لها في الأسواق العالمية أو التي قد تضر بالشركة ضرراً بليغاً إذا ماتم نشر تلك المعلومات .

الجهود الوطنية فى مكافحة جرائم المعلوماتيه:

أن القانون فى مفهوم كثير من الناس ماهو الا تعبيرعن احتياجات المجتمع او هكذا ينبغى ان يكون.ومن ثم فان اوامره ونواهيه ماهى الا تنظيم لما ينشأ فى المجتمع من علاقات ،ولذلك فانه من الطبيعى ان ينشغل ويهتم القائمون على امره بمراجعة النصوص الموجوده كلما جد جديد فى امور المجتمع للاطمئنان على ان هناك ما يواجه القادم الجديد او النظر فيما ينبغى عمله ازاءه ، وليس ذلك من قبيل الوقوف فى وجه القادم الجديد ولكن من باب التحوط لما ينشأ من اشكاليات ،اثر تسارع التكنولوجيات الحديثه وتعامل المجتمع معها ،وتوفر البرامج وتغيير بعض الجرائم الى اشكالها وانماطها المعتاده وتغيير الافعال التى يمكن وضعها فى اطار الافعال الاجرامية مكتملة العناصر،على اقل تقدير من الناحيه النظرية.والتى يمكن كذلك تصنيفها فى اطار فهمنا لها كجريمة فى القانون العام،وذلك لغياب او عدم وجود قانون خاص او عدم مواكبة القانون الموجود حتى يتناول هذه الافعال بالتجريم ذلك لان الحاسب الالى نفسه لم يكن فى تصور او فى ذهن المشرع السودانى حينما وضع القانون الجنائى لسنة 1991م والذى اعقبه صدور قانون خاص بالجريمة المعلوماتية فى العام 2007م.

لذلك ينص المشرع السودانى على مصطلح الارهاب الالكترونى ولكنه اورد لفظ الارهاب فى عدة مواضع وسن لها عقوبات وذلك فى ظل قانون مكافحة الارهاب 2001م،وقانون غسل الاموال وتمويل الارهاب 2010م ، عليه فقانون الجرائم

المعلوماتية هو خطوة نحو تشريع يجب ان يستكمل بتحديث القانون او ان صح التعبير معالجة الناحية الاثباتية في القانون لان قانون الاثبات 1994 لم ولن يعالج مسائل الجرائم المعلوماتية وفي تقديري انه لابد من العمل على سن قانون اثبات للجرائم المعلوماتية والاستفادة من الارشادات الخاصة بالاثبات المعلوماتي.

الجريمة الالكترونية في القانون السوداني :

صدر في السودان قانون جرائم المعلوماتية لسنة 2007م ، ووضع اسس لتجريم الافعال التي تستهدف نظم ووسائط وشبكات المعلومات هذا القانون يعتبر نسبياً من أحدث القوانين العربية من حيث تاريخ صدوره،حيث سعى فيه المشرع الي إستيعاب تجارب الاخرين حسبما ورد في المذكرة التفسيرية له فأخذ بما جاء في القوانين النموذجية العربية وقوانين الدول الغربية وخلافاً لقوانين الدول العربية التي سبقته فقد جرم طائفة واسعة من الافعال ، وفي إطار هذا التجريم نص المشرع على افعال معينة خصها بالذكر وحدد عقوبتها وهي تنحصر في الأتي :-[34]

أولاً : دخول المواقع وأنظمة المعلومات المملوكة للغير

جرم هذا القانون دخول المواقع وأنظمة المعلومات من موظف عام أو أي شخص أخر وفي هذا جرم كل من يدخل موقعاًأو أي نظام معلوماتي دون ان يكون مصرحاً له بالدخول ويقوم بناً على هذا الدخول بالاطلاع عليه او نسخه ،يعاقب على ذلك الفعل بالسجن مدة لاتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً.

أو يقوم بالغاء بيانات او معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغيرها أو إعادة نشرها أو تغير تصاميم الموقع أو إلغائه أو شغل عنوانه ويعاقب القانون من يقوم بذلك الفعل بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة

---

[34] قانون جرائم المعلوماتية لسنة 2007م ، عزة محمد الحسن ، الجريمة المعلوماتية في القانون السوداني مطبوعات جامعة السودان المفتوحة ، ص 14.

أو بالعقوبتين معاً كما جرم أيضاً في إطار هذه الجريمة فعل دخول المواقع وأنظمة المعلومات من موظف عام فعاقب كل موظف عام يدخل بدون تفويض موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغبر بالسجن مدة لاتتجاوز خمس سنوات او بالغرامة أو بالعقوبتين معاً بأعتبارها عقوبة مشددة خاصة بالموظف العام وفقاً لصفة الائتمان المفترضة فيه.

ثانياً: التنصت أو إلتقاط أعتراض الرسائل

جرم المشرع فعل التنصت فكل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما حكمها أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً ، ولم يحدد المشرع الغرض من التنصت أو الاعتراض وكان ينبغي إفراد فقرة خاصة بتشديد العقوبة اذا كان الغرض من هذا الفعل التجسس على الاسرار الحكومية أو العسكرية كما الحال بشأن القانون الامريكي الذى يعاقب بشدة على التجسس على أسرار البنتاجون .

ثالثاً : جريمة دخول المواقع عمداً بقصد الحصول على بيانات أو معلومات أمنية

في هذه الجريمة يعاقب القانون كل من من يدخل عمداً موقعاً أو نظاماً مباشرة أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها بغرض : -

أ- الحصول على بيانات او معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً.

ب- إلغاء بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني أو حذفها أو تدميرها أو تغيرها يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً ، وكأنه اراد سد الخلل في عدم تشديد عقوبة جريمة

التنصت في حال أن الغرض منها هو التجسس وإيقاف او تعطيل او إتلاف البرامج او البيانات او المعلومات في هذه الجريمة عاقب المشرع السوداني كل من يدخل بأي وسيلة نظاماً او وسائطاً او شبكات المعلومات وما في حكمها ويقوم عمداً بإيقافها او تعطيلها او تدمير لبرامج او البيانات او المعلومات او مسحها او حذفها او اتلافها بالسجن مدة لاتتجاوز ست سنوات او بالغرامة او بالعقوبتين معاً وجريمة الاتلاف الالكتروني هي من أخطر انواع الجرائم اذ ان ما يتلف الكترونياً لايمكن اصلاحه بسهولة خاصة اذا كانت المعلومة الالكترونية بين برمجيات معقدة ومرتبطة بأنظمة التشغيل .

ث- إعاقة أو تشويش أو تعطيل الوصول للخدمة .

ج- في هذه الجريمة عاقب المشرع كل من يعوق او يشوش او يعطل عمداً وبأي وسيلة الوصول الي الخدمة او الدخول الي الاجهزة او مصادر البيانات او المعلومات عن طريق شبكة المعلومات او احد اجهزة الحاسوب او ما في حكمها بالسجن مدة لا تتجاوز سنتين او بالغرامة او بالعقوبتين معاً وهي جريمة تفرد بها القانون السوداني لجرائم المعلوماتية اعتبارأن الجاهزية التقنية في توفير جدر الحماية غير متوفرة.

الجرائم الواقعة على الاموال والبيانات والاتصالات وفي هذه الطائفة من الجرائم عاقب المشرع السوداني على ارتكاب جملة من الافعال تطال الاموال اياً كان شكلها والبيانات والاتصالات فعاقب على ارتكاب جريمة التهديد او الابتزاز فكل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب او مافي حكمها في تهديد او ابتزاز شخص لحمله على القيام بفعل أو الامتناع عنه ولو كان هذا الفعل او الامتناع مشروعاً يعاقب باسجن مدة لاتتجاوز سنتين او بالغرامة او بالعقوبتين معاً وعاقب ايضاً على الاحتيال او أنتحال صفة غير صحيحة فكل من يتوصل عن طريق شبكة المعلومات أو اجهزة الحاسوب وما في حكمها عن طريق الاحتيال او استخدام اسم كاذب او

انتحال صفة غير صحيحة بغرض الاستيلاء لنفسه او لغيره على مال او سند او توقيع للسند يعاقب بالسجن مدة لا تتجاوز اربع سنوات او بالغرامة او بالعقوبتين معاً وذلك عاقب كل من فعل الحصول على ارقام او بيانات بطاقات الإئتمان فكل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول الي ارقام او بيانات او معلومات للبطاقة الائتمانية او مافي حكمها بقصد إستخدامها في الحصول بيانات الغير او امواله او ما تتيحه تلك البيانات او الارقام من خدمات يعاقب بالسجن مدة لا تتجاوز خمس سنوات او بالغرامة او بالعقوبتين معاً ايضاً جرم المشرع السوداني في اطار حملته الواسعة لتجريم بعض الاعمال الالكترونية فعل الانتفاع دون وجه حق بخدمات الاتصال فكل من ينتفع دون وجه حق بخدمات الاتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب او مافي حكمها يعاقب بالسجن مدة لا تتجاوز أربع سنوات او بالعقوبتين معاً.

جرائم الارهاب والملكية الفكرية:

هذه الطائفة من الجرائم التي تحتوي على نوعين من الافعال الاولي منها هي أفعال إنشاء أو نشر المواقع للجماعات الارهابية والثانية هي نشر المصنفات الفكرية ففي الافعال الاولي جرم المشرع كل من ينشئ او ينشر او يستخدم موقعاً على الشبكة لترويج افكارها او تمويلها او نشر كيفية تصنيع المواد الحارقة او المتفجرة او اي ادوات تستخدم في الاعمال الارهابية يعاقب بالسجن مدة لا تتجاوز سبع سنوات او بالغرامة او بالعقوبتين معاً ومن المعلوم ان هذه الطائفة من الافعال راج الحديث عنها وتناولها إعلامياً بعد أحداث الحادي عشر من سبتمبر بالولايات المتحدة الامريكية ولما كان الارهاب لا وطن ولادين فقد أحسن المشرع صنعاً بالنص على هذه الجريمة .

أما جريمة نشر المصنفات الفكرية في البيئة الالكترونية فقد جاءت مواكبة للثروة في مجال حماية الملكية الفكرية ولهذا فقد عاقب المشرع كل من ينشر دون وجه حق عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها اي مصنفات فكرية أو أدبية أو أبحاث علمية أو مافي حكمها باسجن مدة لا تتجاوز سنة أو الغرامة أو بالعقوبتين معاً فقط نلاحظ ان المشرع جمع بين جرائم الارهاب الالكتروني وجرائم الملكية الفكرية أدنى رابط يجمع بينهما والرؤية لدينا أن يتم الفصل بينهما .

تطبيقات عملية لإشتقاق الأدلة في الجرائم المعلوماتية:

التزييف والتزوير الرقمي ونحن نعيش الان عصر التزوير الالكتروني وهو أحد الاشكال ، وهو ما اقتضى نشأة مايعرف بالعلم الجريمة الرقمية وما يتطلب اشتقاق الدليل الرقمي الفني الشرعي الرقمي يلاحظ انه في كثير من الاحيان الجريمة الواحدة قد تجمع بين أدلة مادية وأدلة معلوماتية وهذا ما سنعرضه فيما يلى :- [35]

القضية الاولى :

أحالت النيابة العامة قضية لإدارة الادلة الجنائية بوزارة الداخلية متضمنة حرز أوراق العملة السودانية المزيفة فئة عشرون جنيهاً وحرز به أوراق تجمع رزم و أحراز النظام CPU الحاسوب وهو مكون من جهاز الحاسوب محتوياً على وحدة المعالجة المركزية والشاشة ولوحة المفاتيح والفأرة وكذا طابعة حاسوبية وماسح ضوئي ومجموعة من الاقراص المرنة والاسطوانات CD وطلبت النيابة العامة تحديد ما إذا كانت العملات المحرزة هذه مزيفة من عدمه مع تحديد ما إذا كان النظام الحاسوبي تم استخدامه في تزييف العملة المضبوطة من عدمه .

---

[35] خبير فتح الله بصلة –حدود الاثبات العلمي في قضايا التزييف والتزوير –دراسة في المفاهيم والاساليب والاجراءات –دار نوبار للطباعة – مصر -2001م ص 83

وسنركز في هذا العرض على عملية استخلاص الدليل الجنائي الرقمي والربط بينه وبين الدليل الجنائي المادي دون أن نعرض لعملية فحص العملات الورقية ذاتها والتي أثبتنا بأنها بالرغم من التشابهات بينها وبين العملات الورقية الصحيحة المناظرة إلا انها عملات ورقية مزيفة وفق أسلوب التزييف الكلى عن طريق التقليد باستخدام طابعة حاسوبية ملونة تعمل بتقنية نفث الحبر لطباعة كل من الوجه والظهر وذلك على النحو التالي :-[36]

تم تشغيل الجهاز بعد التأكد من صلاحية أجزائه وتم فحص وحدات ومكونات النظام وتسجيل انواعها وتوصيفها واسفرت عملية البحث والفحص للمجموعات البرامجية والملفات الموجودة على القرص الصلب والاقراص المرنة والاسطوانات المدمجة عن الاتي:-

أ- وجود برامج لمعالجة الصور وجه وظهر والتي تعمل في بيئة التشغيل النوافذ (WINDOWS – 95) منها: ADOBE – PHOTOSHOP 5.0,

ب- وجود ملفات وفهارس لصور وجه وظهر عملة ورقية سودانية فئة عشرون جنيهاً ،على القرص الصلب المشغل C.

ت- أن الاقراص المرنة المضبوطة والاقراص المدمجة المضبوطة لم نجد عليها اي برامج.

لوحظ بمجرد توصيل وصلات النظام بالكهرباء (بما في ذلك الطابعة) لاحظنا أن الطابعة تعمل وتخرج منها ورقة طبع عليها مجهة غير مكتمل من العملة الورقية السودانية فئة عشرون جنيهاً مع وجود عمله طباعية مكتملة لثلاث صور لظهر عملة ورقية فئة عشرون جنيهاً بظهر الورقة .

---

[36] نفس المرجع السابق ، ص 85.

وتم تفسير ذلك فنياً وعلمياً با لتقرير بان أخر أمر بالطباعة لم تتمكن الطابعة من إكماله حيث تم فصل الكهرباء بطريقة غير صحيحة عند ضبط أدوات الجريمة .

تم أخذ مخرج طابعي لكل منها من الطباعة المضبوطة ،وهو يمثل تفريغ الدليل الرقمي في شكل مادي وقد تم إيداعها داخل الحرز الرابع بعد التأشير عليها بالنظر وبرقم قيد تقريرنا الحالي .

الربط بين الدليل المعلوماتي الرقمي والدليل المادي :

بعد إجراء التشغيل وعمليتى الفحص والمقارنة بين ورقات العملة الورقية السودانية فئة عشرون جنيهاً المضبوطة والعملة مكتملة الظهر وغير مكتملة طابعة الوجه والتي خرجت من الطابعة المضبوطة بمجرد توصيل وصلات وحدات النظام بالكهرباء (وهما يمثلان الدليل الجنائي المادي) ووجه نظر العملة والورقة السودانية فئة عشرون جنيهاً المحملة على القرص الصلب (هي تمثل الدليل الجنائي الرقمي) ثبت الاتي:-
[37]

أ- ان بيانات العملة الورقية المحملة بالقرص الصلب (المشغل C) بالجهاز (الدليل الجنائي الرقمي) هي ذاتها تحملها ورقات العملة السودانية فئة عشرون جنيهاً (الدليل الجنائي المادي).

ب- الاتفاق في خواص المخرج الطباعي بين ورقات العملة الورقية السودانية فئة عشرون جنيهاً المضبوطة وبين المخرج الطباعي للطابعة للعملة مكتملة الظهر وغير مكتملة طباعة الوجه والتي خرجت من الطابعة المضبوطة بمجرد توصيل وصلات وحدات النظام بالكهرباء هذا من جانب وبين المخرج الطباعي الذي اخذ بمعرفتنا أثناء فحص وتشغيل الجهاز من جانب أخر .

---

[37] نفس المرجع السابق ، ص 89.

ثبت من واقع هذه الفرضية مايلي :-

أ- ان النظام الكمبيوتري المضبوط بمكوناته المادية HARDWARE، وبمكوناته البرامجية SOFTWARE وجد يعمل بتوافق ومهيأ للقيام بالعملية التزييفية .

ب- ان الدليل الجنائي الرقمي المحمل بملفات القرص الصلب (المشغل C) بالجهاز يرتبط ويتكامل مع (الدليل الجنائي المادي) الخاص بالعملية التزييفية لورقات العملة المضبوطة .

يتبين لنا من مجمل هذه الفرضية ان نظم وقواعد الاثبات الجنائي التقليدية المعمول بها قاصرة وإثبات الجرائم المعلوماتية بشكل مباشر ، كما أن الفكر التقليدي غير ملائم لعملية كشف ومكافحة وتحقيق مثل هذا النوع من الجرائم واشتقاق الدليل منها ثم الحكم فيها بل يحتاج ذلك لمحقق معلوماتي وقاضي معلوماتي فضلاً عن الخبير المعلوماتي .

فقانون جرائم المعلوماتية في تقديري الشخصي خطوة في حينها كانت مواكبة وضرورية ولكن بما ان وسائط الاتصالات والتقنيات الحديثة في تطور سريع لابد من وضع قانون يحاول ان يجاري هذا التقدم مع العلم بان الجريمة دائما تسبق القانون ولكن وضع نصوص تتيح للمحاكم القياس عليها لمواكبة التطور مثل عنوان الانترنت كمثال فانه يجب بالقانون الزام مزودي خدمة الانترنت بالاحتفاظ بسجل لمستخدمي الانترنت لفترة معقولة تمكن الرجوع لمرتكب الجريمة اذا كان هناك عنوان انترنت كما يمكن اعتماد ان الجهاز المرتكب منه الجريمة الالكترونية هو الدليل الاول او الحقل الاثباتي الاول الذي يمكن من خلاله اثبات ارتكاب الجريمة واتخاذ ما من شأنه من اجراءات تمكن المحاكم من تسهيل عملها.

الفصل الثانــي

الارهاب الالكتروني

المبحث الاول : ماهية الارهاب

اختلف علماء المسلمين فى مسمى ومصطلح ارهاب واختلاطه مع مصطلح ترويع وهى الاحق بالتسمية حيث تشير كلمة راهب اى خائف معنى له علاقة بالدين والعباد اما مصطلح ترويع فهو الذى بخلاف الامن. عليه من خلال هذا الفصل سنتعرض لمصطلح الارهاب بما يعنى الترويع والذى لا يجوز شرعا العمل به تجاه المجتمعات الاسلامية وغيرها خاصة فى زمن السلم.

الإرهاب لغة:

الإرهاب مصدر أرهب ومادتها رهب الذي مصدره رهب ومعناها (أخاف وأفزع) وقد أطلق لفظ إرهاب للذين ينتهجون طريق العنف لتحقيق أهداف سياسية إما في معنى الخوف والخشية كما في قوله تعالى (ولما سكت عن موسى الغضب اخذ الألواح وفى نسختها هدى ورحمة للذين هم لربهم يرهبون)[38]

(وكما في قوله تعالى (وأياى فأرهبون) [39].

ومعنى الرعب والفزع كما في قوله تعالى (وأضمم إليك جناحك من الرهب) [40] وجاء في معنى الخوف والرعب في القتال والمعارك لقوله تعالى (وأعدوا لهم ما

---

[38] سورة الأعراف الايه 154

[39] سورة البقرة الايه 40

[40] سورة القصص الايه 132

استطعتم من قوه ومن رباط الخيل ترهبون به عدو الله وعدوكم وآخرين من دونهم لا تعلمونهم الله يعلمهم) [41] .

والارهاب يعنى فى اللغات الاجنبيه القديمه مثل اليونانيه :حركه من الجسد تفزع الاخرين.

وقد اقترنت في اللغة العربية بالخوف المقترن بالاحترام وليس الخوف الناتج عن تهديد قوة مادية أو حيوانية أو كوارث طبيعية لأن ذلك يعتبر رعباً أو ذعراً وليس رهبه والخوف من العمليات الإرهابية لا يقترن باحترام للقائمين بالإرهاب لذلك أعتبر التعريف غير صحيح في اللغة العربية لغوياً وإنما هو خوف يعبر عنه بالرعب وليس الرهبة ويجب أن تنتهي إلى الترجمة الصحيحة وهى "إرعاب"[42]

وليس إرهاب ولكن كلمة إرهاب تواتر الناس على ذكرها.

ومن خلال ما تقدم يتبين ان معنى الارهاب فى اللغه يدل على الاخافه والتفزيع والترويع.

الإرهاب في الاصطلاح :

"الإخافة" و"التفزيع" و"الترويع" أما في الاصطلاح فلقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب ويرجع ذلك إلى تنوع أشكاله ومظاهره وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً فقانون مكافحة الإرهاب العماني عرف الإرهاب بأنه كل فعل من أفعال العنف أو التهديد به يقع تنفيذا لمشروع إجرامي فردي أو جماعي ولغرض

---

[41] سورة الأنفال الايه 60

[42] مجمع اللغة العربية– معجم الوسيط– الجزء الأول ص 390

إرهابي عليها أو تعريض أحد الموارد الوطنية للخطر ويكون الغارض إرهابيا إذا كان يهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم أو أغراضهم أو حقوقهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو الاستيلاء أو تهديد الاستقرار أو السلامة الإقليمية للسلطة.

أو وحدتها السياسية أو سيادتها أو منع أو عرقلة سلطاتها العامة عن ممارسة أعمالها أو تعطيل تطبيق أحكام النظام الأساسي للدولة أو القوانين أو اللوائح في حين نجد أن مجمع البحوث الإسلامية بالأزهر يعرف الإرهاب بأنه (ترويع الآمنين وتدمير مصالحهم ومقومات حياتهم والاعتداء على أموالهم وأعراضهم وحرياتهم وكرامتهم الإنسانية بغياً وإفساداً في الأرض) .

أما مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فذهب في تعريفه للإرهاب بأنه: (العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان في دينه ودمه وعقله وماله وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحرابة وإخافة السبيل وقطع الطريق وكل فعل من أفعال العنف أو التهديد يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أموالهم للخطر ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها).

أما بالنسبة للاتفاقية العربية لمكافحة الإرهاب فإنها عرفت الإرهاب بأنه: (كل فعل من أفعال العنف أو التهديد به أياً كانت دوافعه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم

بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر). ومن التعريف السابق نجد أن المشرع العربي قد أرتكز على عنصرين:

1. **مادي** : وهو فعل العنف أو التهديد به أياً كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع أجرامي فردى أو جماعي.
2. **معنوي:** وهو القصد الجنائي

كما عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م الإرهاب بأنه: (الأفعال الإجرامية الموجهة ضد إحدى الدول والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة). إما في السودان فجرائم الإرهاب كما حددها القانون تشمل كل الأفعال التي تحمل نوايا عدائية سواء قام بها الأفراد أو الجماعات، بغرض إشاعة الخوف أو تهديد الحريات أو الأرواح أو أمن الأفراد وتشمل أيضا إلحاق الخسائر بالممتلكات العامة والخاصة والمؤسسات عن طريق احتلالها أو مصادرتها أو الإضرار بها[43] .

تعريف الاتحاد الاوربى عام 2002م بانه:

اعمال ترتكب بهدف ترويع الاهالى او اجبار حكومه او هيئه دوليه على القيام بعمل ما ،او تدمير الهياكل الاساسيه او الدستوري هاو الاقتصادي هاو الاجتماعيه لدوله او هيئه او زعزعة استقرارها .

تعريف الإرهاب في الشريعة الإسلامية:

---

[43] الاتفاقية الدولية لمكافحة الارهاب للعام 1937

يطلق على جريمة الحرابة أو قطع الطريق أو قتل الناس أو إرهابهم وإشاعة الفوضى والرعب من الكبائر المنهي عن اقترافها بالكتاب والسنة والإجماع وهو نية الجاني أو هدفه بإلقاء الرعب بين الناس أو ترويعهم.

أما إذا نظرنا إلى الجريمة حسب القانون الجنائي السوداني لسنة1991 هي (كل فعل يعاقب عليه بموجب أحكام القانون الجنائي أو أي قانون آخر) وتشمل أي تصرف مخالف للقانون بالفعل الايجابي أو بالامتناع السلبي في ظروف يوجب فيها القانون العمل الايجابي وينتج عن ذلك الفعل تهديد خطير لأمن وعافية المجتمع سواء أضر بمصلحة عامة أو فردية . وقد اهتم المشرع في تعريفه للجريمة بتحديد أركانها وعناصرها لما لذلك من أهمية بالنسبة للمحققين الذين يسعون لإثبات أركان وعناصر الجريمة حسبما يحدده القانون وإيجاد العلاقة بين تلك الأركان والشخص المتهم بتنفيذها وتتشابه جريمة المعلوماتية مع الجريمة التقليدية في أطراف الجريمة وهم المجرم ذو الدوافع والضحية والتي قد تكون شخصا طبيعيا أو اعتباريا بينما يكمن الاختلاف الحقيقي بين نوعى الجريمة في أداة ومكان الجريمة ففي الجريمة المعلوماتية تكون الأداة ذات تقنية عالية ولا يتطلب مكان الجريمة انتقال الجاني لمكان المجني عليه انتقالا فيزيائيا حيث تتم أغلب الجرائم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة . ومما سبق فان التعريف الجامع الذي يمكن استخلاصه للجريمة المعلوماتية هو أنها (الأنشطة والأفعال الإجرامية التي تصدر عن إرادة جنائية باستخدام الحاسوب وشبكاته وتقنية المعلومات لأجل الاعتداء على أموال أو أنفس أو عرض أو أي حق آخر يحميه القانون ويجعل الاعتداء عليه جريمة يقرر لها عقوبة أو تدبيرا احترازيا) هذا ونخلص إلى أن

استخدام الإرهاب لأدوات المعلوماتية في الإرهاب لهو من الخطورة بمكان لتعقيدها كما أسلفت.[44]

تتعلق هذه الدراسة باستخدام أطر الأمن السيبرانى وتقنيات الاتصالات وتقانة المعلومات الحديثة للحيلولة دون تنفيذ العمليات الإرهابية ومكافحة الجريمة الإلكترونية لعدة اعتبارات من أهمها تأتى التقدمية المذهلة لهذه التقنيات بتسارع مضطرد مما يجعل من شأنها أن تجعل الإرهاب أكثر غموضاً وقتامه وأصبح يشكل تهديدا للأمن الدولي نظرا لما له من اثأر وخيمة على امن واستقرار المواطنين وازداد وجه الإرهاب قبحا عندما ظهر نوع جديد ألا وهو جريمة الإرهاب الالكتروني وبالتالي هي تعمد على السيطرة عليها من بعد بالإضافة إلى صعوبة اكتشافها ومكافحتها ومواجهتها ويعمد الباحث إلى أن يستجلى خلال الدراسة ماهية تعريف اطر الأمن السيبرانى والجريمة الالكترونية والعمليات الإرهابية وإشكالها ونطاقها والأشخاص المستهدفين من قبل الجماعات الإرهابية باستغلالهم في تنفيذ العمليات بالتقنيات المتطورة أنفة الذكر ودورها في مكافحة الإرهاب .

هذا مع بيان التكييف القانوني للمسئولية المترتبة وفقاً لحزمة المواثيق الدولية والتشريعات الإقليمية والوطنية والعرف الجاري العمل به في هذا المجال.

وجريمة الإرهاب قد تتفق مع الجريمة المنظمة في عناصر استخدام القوه على نحو منظم ومستمر ومتصل وغير مشروع يهدف إلى تهديد النظام العام في الدول إلا أن الفارق الجوهري بينهما يكمن في عنصر الهدف فالجرائم المنظمة غالبا ما تهدف إلى تحقيق مطالب أو أغراض ماليه والجرائم الغالبة بين العصابات المنظمة هي جرائم الاعتداء على الأموال بدافع السعي نحو تحقيق الكسب المادي

---

[44] هيثم عبدالسلام محمد ، مفهوم الارهاب في الشريعة الاسلامية (لبنان : بيروت ، دار الكتب العلمية ، 2005) ص 134.

والحصول على مغانم خاصة ونستطيع أن نتلمس أوجه التباين والتمايز بين الإرهاب والإجرام المنظم .

المسؤولية الجنائية في الشريعة الاسلاميه تعني أن يتحمل الإنسان نتائج الفعال المحرمة التي يأتيها مختارا وهو مدرك لمعانيها ونتائجها فمن اتى فعلا محرما لا يريده كالمكره او المغمى عليه لا يسال جنائيا عن فعله ومن أتى فعلا محرما وهو يريده ولكنه لا يدرك معناه كالطفل او المجنون لايسال أيضا عن فعله وقد عرفت الشريعة الاسلاميه المسؤولية الجنائية بتحمل التبعة حيث لا ينظر إلى الجريمة من حيث نتائجها المادية ولكن ينظر إليه من حيث أهليه مرتكبها لتحمل تبعاتها ومن ثم فان معنى المسؤولية الجنائية في القوانين المعاصرة هو نفس معنى المسؤولية الجنائية في الشريعة الاسلاميه ولما كانت الشريعة الاسلاميه تشترط أن يكون الفاعل مدركا فقد كان طبيعيا أن يكون الإنسان فقط هو محل المساءلة الجنائية لأنه وحده هو المدرك المختار .

وتقوم المسؤولية في الشريعة على ثلاثة أسس :-[45]

1. أن يأتي الإنسان فعلا محرماً .
2. أن يكون الفاعل مختاراً .
3. أن يكون الفاعل مدركاً .

الضرورة :

لا يعد مرتكباً جريمة الشخص الذي ألجأته إلي الفعل حالة ضرورة لوقاية نفسه أو عرضه أو ماله أو نفس الغير أو عرضه أو ماله من خطر جسيم محدق لم يتسبب هو فيه قصداً ولم يكن فى قدرته اتقاؤه بوسيلة أخرى ، بشرط ألا يترتب على

---

[45] نفس المرجع السابق ، ص 136.

الفعل ضرر مثل الضرر المراد اتقاؤه أو أكبر منه ، على أنه لا تبيح الضرورة القتل إلا في أداء الواجب .

لا مسؤليه إلا عن فعل نص القانون على تجريمه لأنه وفقا للقاعدة الاصوليه لا جريمة ولا عقوبة بغير نص وبالتالي لا يعد الفعل جريمة إذا وقع إثناء أداء الواجب اوعند استعمال حق الدفاع الشرعي استعمالا مشروعا . وذلك وفقا لنص المواد(11) (12)(16)(17).

لا يعد الفعل جريمة إذا وقع من شخص ملزم بالقيام به أو مخول له القيام به بحكم القانون أو بموجب أمر مشروع صادر من السلطة المختصة ، أو كان يعتقد بحسن نية انه ملزم به، أو مخول له القيام به لا يعد الفعل جريمة إذا وقع عند استعمال حق الدفاع الشرعي استعمالا مشروعا – ينشأ حق الدفاع الشرعي إذا واجه الشخص خطر اعتداء حال أو وشيك الوقوع على نفسه أو ماله أو عرضه أو نفس الغير أو ماله أو عرضه ، وكان من المتعذر عليه اتقاء الخطر باللجوء إلي السلطة العامة أو بأي طريقة أخرى ، ويجوز له أن يدفع الخطر بقدر ما يلزم لرده وبالوسيلة المناسبة. لا ينشأ حق الدفاع الشرعي في مواجهة الموظف العام إذا كان يعمل في حدود سلطة وظيفته إلا إذا خيف تسبيب الموت أو الأذى الجسيم.

لا يبلغ حق الدفاع الشرعي تعمد تسبيب الموت إلا إذا كان الخطر المراد دفعه يخشى منه أحداث الموت أو الأذى الجسيم أو الاغتصاب أو الاستدراج أو الخطف أو الحرابة أو النهب أو الإتلاف الجنائي لمال أو مرفق عام أو الإتلاف الجنائي بالإغراق أو بإشعال النار أو باستخدام المواد الحارقة أو الناسفة أو السامة . لا يعد جريمة ما نتج عرضاً عن فعل مشروع وقع بحسن نية ونجم عنه ضرر غير

متوقع الحدوث لا يعد الفعل جريمة إذا سبب ضرراً لشخص في جسمه أو ماله متى كان بناءً على رضا صريح أو ضمني من ذلك الشخص.[46]

الارهاب الالكتروني:

وجد الارهابيون مساحة واسعة لبث ونشر افكارهم الباطلة والدعوة الي مبادئهم السئية للمجتمع علي شبكة الانترنت العالمية التي ينطلقون منها بأمان محدود وبأسماء مستعارة عبر مواقعهم ومنتدياتهم النصية والصوتية والمرئية حتي غرف نظام المحادثات الصوتي الكبير المعروف بالبالتوك لم يسلم من اهدافهم الالكترونية لتغذية الفكر الارهابي واصطياد اكبر عدد من الشباب المتعاطفين معه وتجنيدهم لدعمه مالياً ومعنوياً بشتى الوسائل الممكنة تحت عبارة (تفجير نت) و (تفكير كوم) حتي تعليم الطرق والوسائل التي تساعد علي القيام بالعمليات الارهابية وذلك بإنشاء مواقع لتعليم صناعة المتفجرات وطرق الاحتيال وإحراق المؤسسات الحيوية وإبراز أساليب الخطف وتنظيف الاسلحة الخفيفة وإعادة صيانتها فضلاً من الاسعافات الاولية،وطرق اختراق البريد الالكتروني ،وكيفية الدخول علي المواقع المحجوبة ،وطريقة نشر الفيروسات وغير ذلك .

الانترنت مكان اَمن للالتقاء:

إذا كان التقاء الارهابين والمجرمين في مكان معين لتعليم طرق الارهاب والاجرام وتبادل الاراء والافكار والمعلومات صعباً في الواقع فإن الانترنت تسهل هذه العملية كثيراً إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد ويتبادلوا الحديث والاستماع لبعضهم عبر الانترنت ،بل يمكن ان يجمعوا لهم أتباعًا انصاراً عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الانترنت ومنتديات الحوار

[46]- د. يس عمر يوسف ، النظريه العامه للقانون الجنائي السوداني ، لسنة 1991، الدار الجامعية ،الطبعة الثانية ، 1996. ص 89

ومايسمى بغرف الدردشة فإذا كان الحصول علي وسائل إعلامية كالقنوات التلفزيونية والإذاعة صعباً فإن إنشاء مواقع علي الانترنت واستغلال منتديات الحوار وغيرها لخدمة أهداف الارهابين غدا سهلاً وممكناً بل تجد لبعض المنظمات الارهابية آلاف المواقع حتي يضمنوا انتشارً أوسع وحتي لو تم منع الدخول الي بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الاخري يمكن الوصول اليها.

لقد وجد الارهابيون ضالتهم في تلك الوسائل الرقمية في ثورة المعلوماتية فأصبح للمنظمات الارهابية العديد من المواقع علي شبكة المعلومات العالمية الانترنت ،فغدت تلك المواقع من أبرز الوسائل المستخدمة في الارهاب الالكتروني.

جهود الدول الاسلامية في التصدي للارهاب الإلكتروني يعتمد على القرآن الكريم والسنة النبوية المطهرة شريعة وحكماً في جميع شئون الحياة ، ومن هذا المنطلق فإن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة تخضع للاحكام الشرعية المستمدة من الكتاب والسنة وفي ضوء تلك الاحكام تقوم الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الاطراف المختلفة ،كما تقوم الهيئات الامنية والقضائية والحقوقية بتنزيل تلك الاحكام واللوائح علي القضايا المختلفة .

وقد صدرت في أغلب الدول العربية والاسلامية بعض الانظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الالكترونية والارهاب الالكتروني ، ونصت تلك الانظمة علي عقوبات في حال المخالفة لهذه الانظمة والتعليمات واللوائح والضوابط المنظمة لاستخدام شبكة الانترنت والاشتراك فيها ، ومن ذلك :

1- الامتناع عن الوصول أو محاولة الوصول الي اي من انظمة الحاسبات الالية الموصلة بشبكة الانترنت أو الي اي معلومات خاصة و مصادر معلومات دون

الحصول علي موافقة المالكين او من يتمتعون بحقوق الملكية لتلك الانظمة والمعلومات والمصادر.

2- الامتناع عن إرسال أو إستقبال معلومات مشفرة إلا بعد الحصول علي التراخيص اللازمة من إدارة الشبكة المعنية بالخدمة .

3- الامتناع عن دخول الي حسابات الاخرين او محاولة استخدامها بدون تصريح.

4- الامتناع عن إشراك الاخرين في حسابات الاستخدام أو إطلاعهم علي الرقم السري للمستخدم.

5- الالتزام باحترام الانظمة الداخلية للشبكات المحلية والدولية عند النفاذ اليها.

6- الامتناع عن تعريض الشبكة الداخلية للخطر وذلك عن طريق فتح ثغرات أمنية عليها .

7- الامتناع عن استخدام المكثف للشبكة بما يشغلها دوماً ويمنع الاخرين من الاستفادة من خدمتها.

8- الالتزام بما تصدره وحدة خدمات (الانترنت) بمدينة الملك عبدالعزيز للعلوم التقنية من ضوابط وسياسيات لاستخدام الشبكة .

9- ضرورة تكوين جسم يهتم بمجال ضبط واستخدام الانترنت والتنسيق فيما يخص الجهات التي يراد حجبها وله على الأخص مایاتي :-[47]

أ- الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للانترنت والتي تتنافي مع الدين الحنيف والأنظمة .

[47] د . سامي جاد عبد الرحمن واصل ، إرهاب ا لدولة في إطار القانون الدولي العام ، دار النهضة ، الطبعة الأولي ، 2004م ص 56.

ب- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية وهذا الجسم يبين مبادرة الدول الاسلامية وسعيه لتنظيم التعاملات الالكترونية وضبطها.

ولقد بدأ السودان كجزء من هذا الجسم في عقد دورات تدريبية ، هي الاولى من نوعها حول موضوع مكافحة جرائم الحاسب الآَلي بمشاركة مختصين دوليين ، وتقدر تكلفة جرائم الحاسب الآَلي في منطقة الشرق الاوسط بحوالي 600 مليون دولار ، 25% من هذه الجرائم تعرض لها أفراد ومؤسسات في السودان خلال عام 2000م فقط ،وفيما تعمل لجنة حكومية مكونة من وكلاء الوزارات المعنية بهذا الموضوع على الانتهاء من إنجاز مشروع نظام التجارة الالكترونية ، فهي مكلفة أيضاً بوضع النظم والبيانات ، وتقيم البنية التحتية وجميع العناصر المتعلقة بالتعاملات الالكترونية ، وتأتي هذه الاستعدادات للحد من انتشار هذا النوع من الجريمة محلياً فيها خاصة أن العالم يعاني من انتشارها بشكل واسع بعد ان تطورت بشكل لافت للنظر فيما يخص ماهية هذا النوع من الجرائم ومرتكبيها وأنواعها و وسائل مكافحتها إلي جانب الأحكام والانظمة التي تحد من ارتكابها.

وتهدف الاجراءات الي تنمية معارف ومهارات المشاركين في مجال مكافحة الجرائم التي ترتكب عن طريق الكمبيوتر او عبر شبكة الحاسب الآَلي وتحديد انواعها ومدلولاتها الامنية وكيفية ارتكابها وتطبيق الاجراءات الفنية لأمن المعلومات في البرمجيات وأمن الاتصالات في شبكات الحاسب الألي والاجراءات الادارية لأمن استخدام المعلومات ويرتكب هذا النوع من الجرائم بواسطة عدة فئات مختلفة ولعل الفئة الاخطر من مرتكبي هذا النوع من الجرائم هي فئة ممارسو الاجرام المنظم التى يستخدم أفرادها الحاسب الآَلي لأغراض السرقة أو السطو على المصارف والمنشآَت التجارية ،بما في ذلك سرقة أرقام البطاقات الائتمانية والارقام السرية ونشرها أحياناً

على شبكة الانترنت كما تستخدم هذه الفئة الحاسب الآلي لإدارة أعمالها غير المشروعة كالقمار والمخدرات وغسيل الاموال ، وعلى رغم تنوع الفئات التى ترتكب هذه النوعية من الجرائم إلا أن الطرق المستخدمة في الجرية تتشابه في أحيان كثيرة.

ولذلك فإن أجهزة الأمن بحاجة الى الكثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر خاصة في مسرح الجريمة حتى يكون رجل التحقيق قادراً على التعامل مع الادوات الالكترونية من أجهزة وبرامج ، أصبح الارهاب الالكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الارهابيين عبر الانترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم ، وهذه المخاطر تتفاقم بمرور كل يوم لان التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الارهابية الالكترونية والتي سببت أضراراً جسيمة على الافراد والمنظمات والدول . ولقد سعت العديد من الدول إلي اتخاذ التدابير لمواجهة الارهاب الالكتروني الا ان هذه الجهود غير كافية ولا تزال بحاجة الي المزيد من هذه الجهود لمواجهة هذا المارد الخطير.

فالإرهاب الالكتروني أصبح خطراً يهدد العالم بأسره ويكمن الخطر في سهولة استخدام التقنية الحديثه مع شدة أثرها وضررها فيقوم مستخدموها بعملهم الارهابي وهم في منازلهم او مكاتبهم او في المقاهى او حتي من غرفتهم في احدى الفنادق.

عوامل حفظ المجتمع من الإرهاب الالكتروني:

توصل الكثير من العلماء التقنيين الي عوامل تحفظ المجتمع من الارهاب الالكتروني:-[48]

أولاً : أن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة يجب أن تخضع للأحكام الشرعية المستمدة من الكتاب والسنة وفي ضوء تلك الاحكام تقوم

---

[48] نفس المرجع السابق ، ص 61.

الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة كما تقوم الهيئات القضائية والامنية والحقوقية بتنزيل تلك الاحكام واللوائح على القضايا المختلفة وفض النزاعات الناتجة عنها .

ثانياً : ان من أعظم الوسائل المستخدمة في الارهاب الالكتروني إستخدام البريد الالكتروني في التواصل بين الارهابين وتبادل المعلومات بينهم،بل إن كثيراً من العمليات الارهابية التي حدثت في الأونة الاخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بالعمليات الارهابية والمخططين لها.

ثالثاً : إختراق البريد الالكتروني خرق لخصوصية الاخرين وهتك لحرمة معلوماتهم وبياناتهم والله سبحانه وتعالى نهى عن التجسس والشريعة الاسلامية كفلت حفظ الحقوق الشخصية للانسان وحرمت الاعتداء عليها بغير حق ، كما ان الاعتداء على مواقع الانترنت بالاختراق او التدمير ممنوع شرعياً ويعيد تدمير المواقع من باب الاتلاف وعقوبته أن يضمن ما اتلفه فيحكم عليه بالضمان.

رابعا : يقوم الارهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الانترنت لنشر أفكارهم والدعوة الي مبادئهم وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الارهابية فقد أنشئت مواقع لتعليم صناعة المتفجرات وكيفية إختراق وتدمير المواقع وطرق اختراق البريد الالكتروني وكيفية الدخول الي المواقع المحجوبة وطريقة نشر الفيروسات وغير ذلك .

خامساً : حجب المواقع الضارة والتى تدعو الى الفساد والشر ومنها المواقع التي تعلم الارهاب والعدوان والاعتداء على الاخرين بغير وجه حق من الاساليب المجدية والنافعة لمكافحة الارهاب الالكتروني .

سادساً : علي الرغم من إدراك أهمية وجود وتطبيق احكام وانظمة لضبط التعاملات الالكترونية والتي تعتبر وسيلة من وسائل مكافحة الارهاب الالكتروني فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الاحكام لايزال في مراحله الاولية وماتم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية التي لا تستوعب القضايا المستجدة في اعمال تقنية المعلومات كما لا توجد بصورة منظمة ومعلنة أقسام أمنية ومحاكم مختصة ومنتجات اعلامية لشرائح المجتمع المختلفة .

سابعاً : إن اجهزة الامن تحتاج الي كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها وتطوير إجراءات الكشف علي الجريمة خاصة في مسرح الحادث بحيث تتمكن من تقديم الدليل المقبول للجهات القضائية وأيضاً يلزم نشر الوعى العام بجرائم الكمبيوتر والعقوبات المترتبة عليهاواستحداث الاجهزة الامنية المختصة القادرة على التحقيق في جرائم الكمبيوتر والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم .

ثامناً : تضطلع الحكومة السودانية بجهود جبارة في مكافحة الارهاب الالكتروني ولقد أصدرت مجموعة من الانظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الالكترونية والارهاب الالكتروني ، إضافة الي عقد دورات تدريبية هي الاولى من نوعها حول موضوع جرائم الحاسب الآلي بمشاركة مختصين دوليين .

تاسعاً : على مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سنت أنظمة لضبط التعاملات الالكترونية وتضمنت تلك الانظمة عقوبات للمخالفين في التعاملات الالكترونية ومكافحة الارهاب الالكتروني ،واننا من هذ المنطلق ندعو جميع المشايخ وطلاب العلم والكتاب المتمرسين بالمشاركة معنا في دحض الباطل وقمع الزيف ونشر السنة الصحيحة والنصح والارشاد للصواب والرد بالحجة والبرهان علي

ماينشر بين الحين والأخر في الشبكة العنكبوتية من كذب وتلبيس وهذا من الجهاد في سبيل الله تعالى سائلين الله عز وجل المنفعة وبلوغ القصد والله ولي التوفيق.

إستخدام شبكة الإنترنت من قبل المنظمات الإرهابية:

شبكة الانترنت عالم شديد النمو سريع التطوير ونتيجة لذلك فقد تغيرت النظرة على الارهاب الالكتروني والتي كانت منحصرة في الاعمال التخريبية السالفة الذكر واصبحت تشمل أنشطة اكثرة خطورة تمثلت وكما يشر أحد الباحثين المتخصصين في الاستخدام اليومي للانترنت من قبل المنظمات الارهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم فالوجود الارهابي النشط علي الشبكة العنكبوتية هو متفرق ومتنوع ومراوغ بصورة كبيرة فاذا ظهر موقع ارهابي اليوم فسرعان مايغير نمطه الالكتروني ثم يختفي ليظهر مرة بشكل جديد وعنوان الكتروني جديد بعد فترة قصيرة ،وفي نفس الوقت يدعى الارهابيون انهم اصحاب قضايا نبيلة ويشتكون من سوء المعاملة من قبل الاخرين.

ومن الامثلة على بعض المواقع الالكترونية العربية التي قامت بانشائها وتصميمها بعض التنظيمات الارهابية مايأتي :-

أ- **موقع النداء :** وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبرعام 2001م ومن خلال تصدر البيانات الاعلامية للقاعدة .

ب- **ذروة السنام :** وهي صحيفة اليكترونية دورية للقسم الاعلامي لتنظيم القاعدة.

ت- **صوت الجهاد :** وهي مجلة نصف شهرية يصدرها مايسمى بتنظيم القاعدة في جزيرة العرب وهي تصدر بصيغتي (Word)،(Pdf) وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظرية .

ث-**البتار** : وهي مجلة عسكرية اليكترونية متخصصة تصدر عن تنظيم القاعدة وتختص بالمعلومات العسكرية والميدانية والتجنيد .

ومن أهم العناصر الأساسية لاستخدام الانترنت في أغراض أرهابية: [49]

أ- **التنقيب عن المعلومات :**

إن شبكة الانترنت في حد ذاتها تعتبر مكتبة الكترونية هائلة الحجم وتكتظ بالمعلومات الحساسة التي يسعى الارهابيون للحصول عليها مثل أماكن المنشأت النووية والمطارات والمعلومات المختصة بسبل مكافحة الارهاب وبذلك يكون 80% من مخزونهم المعلوماتي معتمداً في الاساس علي مواقع الكترونية متاحة للكل ،دون خرقاً لأي قوانين أو بروتوكلات الشبكة

ب- **الاتصالات** : تساعد شبكة الانترنت المنظمات الارهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها وذلك نظراً لقلة تكاليف الاتصال باستخدام الانترنت مقارنة بالوسائل الاخرى ،كما انها تمتاز بوفرة المعلومات التي يمكن تبادلها وقد أصبح عدم وجود زعيم ظاهر للجماعة الارهابية سمة جوهرية للتنظيم الارهابي الحديث ، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الارهابية وكل هذا سبب سهولة الاتصال والتنسيق عبر الشبكة العالمية .

ت- التعبئة وتجنيد إرهابين جدد :

إن استقدام عناصر جديدة داخل المنظمات الارهابية يحافظ على بقائها واستمرارها وهم يستغلون تعاطف الاخرين من مستخدمي الانترنت مع قضاياهم ويجتذبون هولاء السذج بعبارات براقة وحماسية من خلال غرف الدردشة الالكترونية ونحن نعلم أن تسلية الشباب والمراهقين هي الجلوس بالساعات الطويلة في مقاهي الانترنت للثرثرة مع جميع أنواع البشر في مختلف أنحاء العالم .

---

[49] سامي جاد عبد الرحمن واصل ، مرجع سبق ذكره ، ص 86.

ث- إعطاء التعليمات والتلقين الالكتروني :

يمتلئ الانترنت بكم هائل من المواقع التي تحتوي على كتيبات وارشادات تشرح طرق صنع القنابل والاسلحة الكيماوية الفتاكة وعند استخدام محرك البحث غوغل(Google) عام 2005م للبحث عم مواقع تضم في موضوعاتها كلمات مثل (إرهابي terrorist) أو (دليل handbook) فكانت نتائج البحث مايقرب من ثمانية الاف موقع .

ج- التخطيط والتنسيق :

تعتبرشبكة الانترنت وسيلة للاتصال بالغة الاهمية بالنسبة للمنظمات الارهابية ،حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات ارهابية محددة ويضيف ويمان أن أعضاء منظمة القاعدة البارزين إعتمدوا بشكل مكثف علي الانترنت في التخطيط لهجمات 11 سبتمبر ويستخدم الارهابيون الرسائل الالكترونية العادية وغرف الثرثرة لتدبير الهجمات الارهابية وتنسيق الاعمال والمهام لكل عنصر إرهابي .

ح- الحصول على التمؤيل :

يستعين الارهابيون ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الالكترونية ،في التعرف على الاشخاص ذوي القلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات مالية لاشخاص اعتباريين يمثلون واجهة لهولاء الارهابيين ويتم ذلك بواسطة البريد الالكتروني بطريقة ماكرة لا يشك فيها المتبرع بأنه يساعد إحدى المنظمات الارهابية .

أشكال العمليات الإرهابية:

تثير ظاهرة الإرهاب اهتمام الشعوب والحكومات في كل دول العالم، نظراً لما لها من آثار وخيمة على أمن المواطنين واستقرارهم، وعلى الإمكانات الاقتصادية والهيبة السياسية للدولة في محيطيها الإقليمي والدولي وتتجلى مظاهر هذا الاهتمام فيما تعدّه الجهات الرسمية بالدولة من خطط إستراتيجية وتكتيكية لمواجهة الإرهاب والقضاء عليه، كما تتجلى في اهتمام المراكز العلمية والمنابر الإعلامية بتناول تلك الظاهرة عبر البحوث والدراسات، والبرامج واللقاءات لبيان أبعادها وآثارها وتبيان ما يستخدم فيها من وسائل وأساليب وأدوات، وما يستحدثه الإرهابيون في هذا الشأن، مستغلين ما تفرزه التقنية الحديثة (التكنولوجيا) من أفكار وآليات في مختلف المجالات، وبخاصة في مجالي الاتصالات والمواصلات، والأسلحة والمتفجرات. ولا بد لنا أن نوضح أثر التطور التكنولوجي على الإرهاب فنحن في السودان في أمس الحاجه لهذه العلوم الحديثة .

وليس هناك أمان وسلامه أكثر من الوقاية والخطوات الاستباقيه والتدريب والتأهيل والاستعداد خصوصا أن الإرهاب أصبح وسيله لتحقيق غايات وأهداف بعض الدول ويمكن أن يتم التدخل في الحدود الجغرافية لتنفيذ عمليات إرهابيه وعند ذلك تكون الاجهزة المختصة على أهبة الاستعداد للتصدي والعمل الايجابي فهو خير من معالجة الآثار السالبة التي يخلفها الإرهاب ويكون الاستعداد بوجود الاجهزة والمعدات الالكترونية الخاصة بالتتبع والمراقبة والرصد بكل أنواعه سوى كان رصدا للاجهزه المخرب هاو الاجهزة التي يتم التحكم بها عن بعد وبوسائل التامين الخاصة بالأماكن ألاستراتيجيه والحيوية في البلاد وهذه الحراسة لها عدة اشكال خلاف الحراسة والتامين بوجود الأفراد اى الوجود الفيزيائى أيضا الحراسة والتامين الالكتروني . تتعدد الأهداف التي تسعى إليها الحركات الإرهابية ويمكن أن نميز من

هذه الأهداف بين الأهداف الأيديولوجية والانفصالية والإجرامية وعلى أساس ذلك تتعدد أشكال الإرهاب على النحو التالي:-[50]

1-المؤسسة أو الإرهاب المؤسسي أو السلطوي نظرا لأنه يحافظ على السلطة الشرعية أو المؤسسات فقد يطلق عليه الإرهاب من أعلى أو الإرهاب الأحمر ولكن ليس كل عنف تمارسه الدولة يسمى إرهابا.

2- الإرهاب الداخلي قد يكون من خلال التعسف في السلطة مثل أعمال التعذيب والمعاملة اللا إنسانية أو التطبيق التعسفي للقوانين وهو ما يطلق عليه أيضا الإرهاب القمعي الذي تحكم من خلاله الدولة سيطرتها على بعض الفئات والحركات الثورية وتتمكن من إسكات المعارضين وذلك من خلال مجموعات إرهابية تؤسسها الدولة لزرع الرعب في أواسط مجموعة معينة من المواطنين أو ضد المجتمع بأسره فبالرغم من أن الرعب اصطلاحا يختلف عن الإرهاب إلا أننا نجد القاسم المشترك بينهما هو الإخضاع بالقوة أما على المستوى الخارجي فالدولة تمارس الإرهاب على صورتين أحدهما مباشر والأخر غير مباشر فالصورة المباشرة على المستوى الخارجي تتمثل في تلك العمليات التي تنفذها وحداتها العسكرية ضد المدنيين في دولة أخرى وبالرغم من انه تعدى عسكري تحرمه قواعد القانون الدولي إلا انه يعد إرهابا ويسمى بالإرهاب العسكري وهو يختلف عن الإرهاب القهري من حيث الهدف حيث يهدف الإرهاب القهري إلى تجميع الشعب والسيطرة عليه في حين يهدف الإرهاب العسكري إلى تفريق الشعب وإضعاف إرادته.

---

[50] لواء الدكتور حسنين المحمدي بوادي، إرهاب الإنترنت، الخطر القادم، القاهرة : الدار الجامعية 2006م ، ص 46.

3- أما الصورة الغير المباشرة فتتمثل في المساعدات التي تقدمها الدولة إلى الإرهاب وجماعاته مثل توفير السلاح والمأوى إلى غير ذلك فدعم الإرهابيين يعتبر إرهاباً.

إرهاب الأفراد والجماعات :

يطلق البعض على الإرهاب الفردي إرهاب التمرد ويشكك في كونه إرهابا للضعفاء ويشير إلى أن المقصود بالضعف هو قلة موارد من يلجئون إلى الإرهاب بشكل كبير عن الموارد التي يتحكمون فيها مقارنة بطموحاتهم فهو لا يعكس ضعفا بقدر ما يعكس مبالغة في الطموح والأهداف ويطلق على هذا النوع من الإرهاب " الإرهاب من أسفل".

أما حركات التحرر التي تستهدف التحرير من الاستعمار والحصول على استقلالها وممارسة حقها في تقرير مصيرها الأمر الذي دفع المجتمع الدولي إلى الاعتراف بشرعية كفاحها في حين أن الحركات الانفصالية لا تستهدف وحدة الدولة وسيادتها الإقليمية ومن ثم لا تعترف بها المواثيق الدولية لأنها تتنافى مع مبدأ وحدة إقليم الدولة المعترفة به دوليا وهذا النوع من الإرهاب يقتصر على الأفراد والمجموعات السياسية ولا يتصور أن تمارسه الدولة اللهم إلا بطريق غير مباشر من خلال دعم بعض الحركات الانفصالية وهو يقوم بصفة أصلية على أسس عرقية أو قومية ويتميز بالعنف الدموي والاستمرارية وله امتداد بين فئات الشعب ومن أمثلته الراهنة منظمة الجيش الجمهوري الإيرلاندي(LIRA) ومنظمة آيتا الانفصالية في إسبانيا التي تطالب بانفصال إقليم الباسط عن إسبانيا ولا توجد حركة قومية أو عرقية انفصالية تمكنت من تحقيق أهدافها حتى الآن من خلال الإرهاب أو بدون استخدامه.

الإرهاب الإجرامي:

إن هذا النوع من الإرهاب تحركه دوافع أنانية وشخصية واقتصادية واجتماعية ويتخذ أساليب متعددة لتحقيق أهدافه مثل الابتزاز والسطو المسلح وأخذ الرهائن لطلب الفدية والتخريب ونهب الأموال والممتلكات وممارسة أعمال الاتجار في المخدرات وعمليات غسل الأموال القذرة و الفساد وغيرها وهو نفس الإرهاب العادي.فقد تعددت أشكال العمليات الارهابيه وبالرغم من إنها في تقديري عمليات إرهابيه تقليديه إلا أنها في تطور مستمر ويمكن إدخال التقنيات التكنلوجيه الحديثة عليها وهذا بدون شك يجعل مكافحتها صعبه ومن أمثلتها :[51]

1. تدمير الأبنيه والمرافق العامة والهامة والاستراتيجية.
2. استخدام المتفجرات لتدمير المرافق الاستراتيجية .
3. اغتيال الشخصيات الهامة.
4. خطف الطائرات.
5. عمليات احتجاز الرهائن.

الإرهاب النووي:

وهنا لابد لي أن أشير إلى اعتراض إسرائيل السفن الحرية التي حاولت فك الحصار عن قطاع غزة في فلسطين نوعاً من الإرهاب ولا بد من توضيح إلى أن حماية الشخصيات الهامة في السودان والوسائل الحديثة والطرق المبتكرة والمتمشية مع التكنولوجيا هي من النتائج والتوصيات التي سوف تقدمها هذه الدراسة وذلك لعدة أسباب من أهمها أن الشخصيات الهامة في السودان غير محمية بسبل علميه تكنولوجيه إلكترونيه متطورة.

---

[51] الفكى احمداى ، القانون الدولي لمكافحة الإرهاب الطبعه 1، القاهرة : دار النهضة ، ب ،ن) ص 142.

الإرهاب والإسلام :

تبيَّن لي من خلال استقراء بعض المعاجم العربية الأصلية أنها قد خلت من كلمة إرهاب ، وهي كلمة أقرها المجمع اللغوي وجذرها (رهب) بمعنى خاف فمعانيها تدور حول الخوف والتخويف ويعرّف (جورج ليفاسير) الإرهاب بأنه : الاستعمال العمدي والمنتظم لوسائل من طبيعتها إثارة الرعب بقصد تحقيق أهداف معينه . قال القرطبي : ترهبون به عدو الله وعدوكم من اليهود والكفار ومشركي العرب فالله جل وعلا يأمر هذه الأمة أن تعد العدة لتخويف هذه الطوائف من الناس ليشعروا بالرعب والهلع من المسلمين كما يشعر الكثير منا الآن من الهلع والخوف من دولة تعداد سكانها مثل تعداد حي من أحياء القاهرة وحين نتأمل في حياة النبي صَلَّى اللَّهُ عَلَيْهِ وآله وَسَلَّمَ نجد أنه طبق الإرهاب في عدد من المرات فنذكر منها.

تخويف أهل مكة وبيان أنه أرسل لإرهابهم فقد قال صَلَّى اللَّهُ عَلَيْهِ وآله وَسَلَّمَ:

(يَا مَعْشَرَ قُرَيْشٍ أَمَا وَالَّذِي نَفْسُ مُحَمَّدٍ بِيَدِهِ لَقَدْ جِئْتُكُمْ بِالذَّبْحِ) أخرجه أحمد وكان يشير إلى عنقه كما في بعض الروايات فهو إرهاب لهم وبيان أنه أرسل ليذبحهم.[52]

الأمر بالاغتيالات ونذكر منها:

خبر اغتيال محمد بن مسلمة لكعب بن الأشرف اليهودي وخبر اغتيال عبد الله بن أنيس لخالد بن سفيان بن نبيح الهذلي . وخبر اغتيال خمسة رجال من بني سلمه من الخزرج يقودهم عبد الله بن عتيك لسلام بن أبي الحقيق . وخبر إرسال النبي . صَلَّى اللَّهُ عَلَيْهِ وآله وَسَلَّمَ . لعمرو بن أمية الضمري وسلمه بن أسلم لقتل أبي سفيان

---

[52] هذا الحديث رواه أحمد في " المسند " (609/11) طبعة مؤسسة الرسالة من رواية الصحابي عبد الله بن عمرو بن العاص رضي الله عنهما ، وحسنه المحققون ، والشيخ أحمد شاكر في تحقيق المسند أيضا ، وحسنه الهيثمي في " مجمع الزوائد " (19/6) ، وكذا الشيخ الألباني في " صحيح الموارد " (1403)

بن حرب ولم يقدرا عليه فقتلا عثمان بن مالك بن عبيدا لله التيمي . وقد قال النبي . صَلَّى اللَّهُ عَلَيْهِ وآله وَسَلَّمَ . لبياميين بن عمير بن كعب لقد آذانا ابن عمك يريد عمرو بن جحاش فجعل جعلا لرجل فقتله وقد أذن له النبي . صَلَّى اللَّهُ عَلَيْهِ وآله وَسَلَّمَ . بذلك . ولم يكتفِ النبي . صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ . بقتل الرجال بل أمر بقتل عصماء بنت مروان وكانت عصماء عند يزيد بن زيد بن حصن الخطمي وكانت تعيب الإسلام وتؤذي النبي وتحرض عليه وتقول الشعر فجاءها عمير بن عدي في جوف الليل حتى دخل عليها بيتها وحولها نفر من ولدها منهم من ترضعه في صدرها فجسها بيده وكان ضرير البصر ونحى الصبي عنها ووضع سيفه على صدرها حتى أنفذه من ظهرها . هذه بعض الاغتيالات التي أمر بها النبي . صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ . وهي نوع من الإرهاب كذلك فكانت الاغتيالات سنة لنا وشريعة. ولو طبقت هذه الطريقة مع عدد ممن أساء إلى الإسلام من أمثال سلمان رشدي وغيره من الكفرة والعلمانيين لوضعنا حدا لمن يتجرأ على دين الله جل وعلا وخبر ذبح النبي صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ لبني قريظة معلوم مشهور فقد ذبح من بلغ منهم وسبى نسائهم وقسّم أموالهم . وقد نجد غير هذه الأمثلة مما يدل على إرهاب النبي صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ للكفرة الفجرة.

ولمن كان هذا الإرهاب ولم كان هذا الإرهاب ؟؟ولكن هذا الإرهاب في ديننا لم يكن إلا مع من اشتهر بعداء الإسلام فهو . صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ . بيّن لقريش لما أكثروا عليه من السب والسخرية أنه سيذبحهم ، وكذا أمر باغتيال من أكثر الطعن في الإسلام وكان رأسا في الكفر ، وقتل بني قريظة لما نزلوا على حكم حليفهم سعد بن

معاذ . رَضِيَ اللَّهُ عَنْهُ . وقبلوا بحكمه من جهة ثم أنهم خانوا العهد واخلفوا الوعد كما هي عادة يهود .[53]

إلارهاب في الإسلام نوعان:

ممدوح : وهو تخويف العدو خشية اعتدائه على المسلمين ، واحتلال ديارهم، ويكون ذلك بالاستعداد الكامل بالتسلح بالإيمان ، والوحدة ، والسلاح ، وقد سبق في آية الأنفال ما يوضح أنه واجب على المسلمي والإسلام ليس بدعاً في هذا الأمر ، فها هي الدول تتسابق في الصناعات العسكرية ، وفي التسلح بالأسلحة التدميرية ، وبإنشاء الجيوش الجرارة ، وبعمل الاستعراضات العسكرية لجنودها وأسلحتها ، وكل ذلك من أجل إظهار قوتها ؛ لإخافة جيرانها ، وأعدائها ، من أن تسول لهم أنفسهم الاعتداء عليها.

مذموم : وهو تخويف من لا يستحق التخويف ، من المسلمين ، ومن غيرهم من أصحاب الدماء المعصومة ، كالمعاهدين ، والمستأمنين ، وأهل الذمة وقد عرَّف " المجمع الفقهي الإسلامي الإرهاب بأنه(العدوان الذي يمارسه أفراد أو جماعات ، أو دول ، بغياً على الإنسان دينه ، ودمه ، وعقله ، وماله ، وعرضه)ويشمل صنوف التخويف ، والأذى ، والتهديد ، والقتل بغير حق ، وما يتصل بصور الحرابة ، وإخافة السبيل ، وقطع الطريق ، وكل فعل من أفعال العنف، أو التهديد ، يقع تنفيذاً لمشروع إجرامي ، فردي ، أو جماعي ، يهدف إلى إلقاء الرعب بين الناس ، أو ترويعهم بإيذائهم ، أو تعريض حياتهم ، أو حريتهم ، أو أمنهم ، أو أحوالهم للخطر ، ومن صنوفه : إلحاق الضرر بالبيئة أو بأحد المرافق ، والأملاك العامة ، أو الخاصة، أو تعريض أحد الموارد الوطنية ، أو الطبيعية ، للخطر ، فكل هذا من

---

[53] د. علي حسن الطوالبة ، مفهوم جرائم الإرهاب في ضوء التشريعات العربية الحديثة ،مركز الإعلام الأمني .

صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها في قوله (ولا تبغ الفساد في الأرض إن الله لا يحب المفسدين) صدق الله العظيم.[54]

وجاء في البيان التنبيه إلى أمرين مهمين :

الأول : الرد على من وصف الإسلام بأنه دين إرهاب فمما جاء فيه :وقد لحظ أعضاء " المجمع " أن الحملات الإعلامية مدبرة ، وهي تنطوي على أباطيل ، وترهات ، تنطلق من إعلام موتور ، معادٍ ، تسهم في توجيهه مؤسسات الإعلام الصهيوني ؛ لتثير الضغائن ، والكراهية ، والتمييز ، ضد الإسلام والمسلمين ، وتلصق بدين الله الخاتم التهم الباطلة ، وفي مقدمتها تهمة " الإرهاب " واتضح لأعضاء " المجمع " أن لصق تهمة الإرهاب بالإسلام عبر حملات إعلامية إنما هو محاولة لتنفير الناس من الإسلام ، حيث يقبلون عليه ، ويدخلون في دين الله أفواجاً. ودعا أعضاء " المجمع " رابطة العالم الإسلامي ، وغيرها من المنظمات الإسلامية ، وكذلك عامة المسلمين إلى الدفاع عن الإسلام ، مع مراعاة شرف الوسيلة التي تتناسب ، وشرف هذه المهمة".

وبينوا في سياق ردهم على الافتراء على الإسلام ، ولصق تهمة الإرهاب به "أن الإرهاب ظاهرة عالمية ، لا ينسب لدين ، ولا يختص بقوم ، وهو سلوك ناتج عن التطرف الذي لا يكاد يخلو منه مجتمع من المجتمعات المعاصرة ، وأوضحوا أن التطرف يتنوع بين تطرف سياسي ، وتطرف فكري ، وتطرف ديني ، ولا يقتصر التطرف الناتج عن الغلو في الدين على أتباع دين معين ، وقد ذكر الله سبحانه وتعالى غلو أهل الكتاب في دينهم ، ونهاهم عنه ، فقال في كتابه الكريم : (قل يا

[54] سورة القصص الايه(77)

أهل الكتاب لا تغلوا في دينكم غير الحق ولا تتبعوا أهواء قوم قد ضلوا من قبل وأضلوا كثيراً وضلوا عن سواء السبيل) .[55]

والثاني : ذِكرهم أن من الإرهاب إرهاب الدول ، والذي سكتت عنه وسائل الإعلام العالمية ، ولم تفضح أهله ، ومما جاء في البيان :"ويؤكد المجمع أن من أنواع الإرهاب : إرهاب الدولة ، ومن أوضح صوره ، وأشدها شناعة : الإرهاب الذي يمارسه اليهود في فلسطين ، وما مارسه " الصرب " في كلٍّ من البوسنة ، والهرسك ، وكوسوفا ، واعتبر " المجمع " أن هذا النوع من الإرهاب : من أشد أنواعه خطراً على الأمن ، والسلام في العالم ، واعتبر مواجهته من قبيل الدفاع عن النفس ، والجهاد في سبيل الله" .أما الإرهاب عند الغرب : فهو ما نقرؤه ، ونشاهده ، من احتلالهم للدول الضعيفة ونهبهم لخيراتها ، وما نراه من التعذيب ، والاغتصاب ، والقتل ، وكل ذلك موثق بالصوت والصورة ، في وثائق لا يمكن إنكارها ، وهو استمرار لتاريخهم القديم في احتلال الدول بالقوة ، والبطش ، والسلاح.والعجيب حقا أن الدول الغربية وخاصة أمريكا لم يضعوا إلى ألان تعريفا للإرهاب وواضح أنهم سيدينون أنفسهم باى تعريف يختارونه ولذلك جعلوا أللفظه مبهمة المعنى فتتصرف إلى من يريدون إلصاق التهمه به . الكفار من قديم يحاربون الإسلام ، ويصفونه بأقبح الصفات ؛ تنفيراً منه (يُرِيدُونَ أَن يُطْفِؤُواْ نُورَ اللَّهِ بِأَفْوَاهِهِمْ وَيَأْبَى اللَّهُ إِلاَّ أَن يُتِمَّ نُورَهُ وَلَوْ كَرِهَ الْكَافِرُونَ) .[56] ، ومن ذلك وصفهم له بالإرهاب ، والوحشية ، وينسون أن الإرهاب ، والوحشية ، وقتل الشعوب ، والتسلط على الخلق بغير الحق ، وكل صفات الذم. إنما هي في دين الكفر ومن صفات الكفار.

وكون بعض المنتسبين إلى الإسلام تصدر منهم بعض التصرفات الخاطئة إما عن جهل أو عن قصد سيئ ، فإن ذلك لا ينسب إلى الإسلام ؛ لأن الإسلام

[55] سورة المائدة الايه77
[56] سورة التوبة الايه 32

ينهى عن ذلك وطريق الخلاص من هذا الاتهام السيئ للإسلام أن يُبَيَّن أن فعل هؤلاء الأشخاص ليس من الإسلام ، وإنما هو تصرف شخصي ، وأن كل مسلم فهو عرضة للخطأ ، وليس هناك معصوم إلا رسول الله صلى الله عليه وسلم.[57]

المبحث الثانــي : القضاء على الإرهاب الإلكتروني

نظراً للتطور الرهيب والمتنامي في مجالات الانترنت وتكنولوجيا المعلومات فإن الارهابيين اصبحوا أكثر اعتماداً على تكنولوجيا الاتصالات الالكترونية وظل الارهاب اكثر تعقيداً وخطورة وهناك كثره في حجم الاخطار الحالية وبالضروره مواجهة تلك التحديات بشيء من الرؤية وحسن التصرف مع ملاحظة ان الارهابيون يجيدون استخدام تلك الشبكة بكفاءة عاليه وبها يستطيع صانعو السلام استخدام الانترنت لمجابهة هذا العمل والمقصود هو نشر الافكار السامية والمتحضرة التي تدعو الي السلام والمحبة والتعايش السلمي بين الحضارات المختلفة وبالتالي تطغي تلك المواقع الصالحة على السموم التي تنشرها المواقع الالكترونية الارهابية ،تلك الانشطة التي تدعم الدبلوماسية وادارة الازمات السياسية بالطرق السلمية عبر الشبكة العالمية للانترنت ،كما أنه لا بد وأن تسعي الدول والحكومات الي فرض الرقابة الكافية على كل مايقدم من خلال الشبكة لمنع الدخول على بعض المواقع التي تبث الفكر الارهابي ،كما هو الحال في المملكة المتحدة حيث وضعت الحكومة البريطانية خططاً للتصدي للارهاب على شبكة الانترنت قدرت تكلفتها بحوالي 500 مليون جنية استرليني هذا بالنسبة للقسم الثاني والاخطر .

لا شك أن مطوري تكنولوجيا المعلومات وخبراء الانترنت مطالبون بملاحقة أنشطتهم التوسعية بأنشطة حماية وسد ثغرات لحماية هذا الفضاء الحيوي من ان يصبح ساحة ارهاب دامية ،ويجب ان يهتم المجتمع الدولي بإبرام اتفاقيات تقنن

---

[57] من فتاوى الفوزان " (1 / 416 ، السؤال رقم 247 13

التشريعات اللازمة لمكافحة تلك الجرائم وتنظم الجهود الدولية لمحاربتها،بما في ذلك بحث إنشاء (نظام للإنذار المبكر من الهجمات الالكترونية) وتطوير برامج أمنه وزيادة وعي المسؤولين التنفيذيين والعملاء بالحاجة الي اجراءات أمنية أفضل

ويجب تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الالكترونية وتوفير التقنيات اللازمة لمواجهتها عبر تطوير أمن شبكات الحاسب باستخدام أنظمة التشفير المتقدمة (والجدران النارية)في الشبكات وانظمة اكتشاف المخترقين عالية الدقة ،والبرامج المضادة للفيروسات كما و أن إنشاء إدارات لمكافحة الارهاب الالكتروني في أنظمة الامن خصوصاً في الدول التي تشهد تقدماً مطرداً اعتمادها على تكنولوجيا المعلومات أمر حيوي خاصة وأن التطور الحاصل في هذا المجال يتسارع والثغرات التكنولوجية فيه تتسع وهو الأمر الذي يستلزم مواجهة كفؤة متخصصة للحد من احتمالات نجاح التهديدات الارهابية في هذا المجال.

مما سبق يتضح لنا أن العالم دولاً وشعوب اصبح امام تحد كبير يتطلب تنسيقاً الكترونياً عالي المستوي بين الاجهزة الامنية في كافة الدول ،فضلا تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذه المشكلة وبخاصة الانتربول لمواجهة كافة اشكال جرائم الارهاب علي الانترنت،ليس هذا فحسب بل ينبغي على المشرع العماني تجريم استخدام شبكة الانترنت في عمليات ارهابية حيث أن القانون الجزائي جاء خالياً وقانون الارهاب وهو من القوانين الحديثة أيضاً جاء خالياً.

في الماضي كان الارهاب TERRORISING يعني قيام بعض الارهابيين بتفجير قنبلة في مكان ما او اغتيال شخصية ما او تفجير طائرة في الجو وما الي ذلك من عمليات روتينية اعتاد رجل الامن في جميع الدول على مواجهتها،اما الان ومع التقدم التقني MODERN TECHNIQUESومع تقدم وسائل الاتصالات الذي نعيشة ونكاد نلمسه فقد تغيرت وتطورت تلك الاساليب التي يحاول الارهابيون بها

الوصول الي اهدافهم فقد اصبح الارهاب الالكتروني هو السائد حالياً واصبح اقتحام المواقع وتدميرها وتغير محتوياتها والدخول علي الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها او الدخول علي شبكات الطاقة او الشبكات الاتصالات بهدف تعطيلها عن العمل اطول فترة ممكنة او تدميرها نهائياًاصبح هو اسلوب الارهاب حالياً في محاولة الوصول الي اغراضهم.

ونحن نرى الان ان الارهاب الذي تمارسه اسرائيل ضد الشعب الفلسطيني لايتمثل فقط في اغتيال رموزه بل وافراد شعبه وتشريد شعبه واستيلاء على ارضه وممتلكاته وما الي ذلك وانما الارهاب الذي دولة اسرائيل امتد ليشمل الارهاب الالكتروني في المواقع الفلسطينية على شبكات الانترنت تتعرض وبصفة مستمرة من الاسرائليين الي الاقتحام والعبث بمسحتوياتها وازالة ماعليها من معلومات وعرض صورة العلم الاسرائيلي على الصفحة الرئيسية بالمواقع المقتحمة وفي المقابل يحاول الفلسطينيين معالجة تلك الاثار وتصحيح وازالة العبث الواقع علي مواقعهم وايضاً يحاولون اقتحام بعض المواقع الاسرائيلية و وضع العلم الفلسطيني على الصفحة الرئيسية بها في المقابل .

وهذا الارهاب لاتقتصر ممارسته على الاسرائيليين الموجودين باسرائيل فقط وكذلك الفلسطينين الموجودين بداخل فلسطين فقط وانما امتد الوضع ليشمل كل الاسرائيليين والفلسطينيون يحاولون مساعدة ذويهم بالدخل – داخل فلسطين في مقاومة الاحتلال الاسرائيلي وقد وفرت لهم شبكة الانترنت التي الغت الحدود الجغرافية بين الدول ،وتلك المساعدة التي اصبح في امكانهم القيام بها من خارج حدود دولتهم وهو ما ساعد كثيرا الفلسطينيين الموجودين بداخل فلسطين المحتلة فبعد ان كانوا بمفردهم وجهاً لوجه مع المحتل اصبحوا يجدون المعاونة الخارجية المؤثرة والمفيدة لهم .

الإرهاب عبر أدوات التواصل الاجتماعي:

نماذج الارهاب المتنوعة الإغارة على مواقع الاخرين وسرقة معلوماتهم وصورهم و وضع تلك الصورة في مواقف مخلة بالاداب وتيديد اصحابها للقبول بعلاقة (في حالة النساء) او طلب المال في حالة النساء والرجال ؟ وهذا ما جعل صائد النساء علي علي مواقع التواصل الاجتماعي يقع فى أيدي شرطة دبي بعد أن استدرجته وفق كمين محكم حتي ضبط المتهارا قانونياً واشار المسؤول التونسي الي وجود جماعات متطرفة على الانترنت تحاول استمالة الناس أو تمرير ثقافة الموت اليهم.

وفي كثير من الدول ترصد هاشتاقات تحريضية علي تويتر وتسجيل ملايين المشاركات أغلبها مجهولة المصدر.

وفي بلاد الغرب ذكرت المصادر أن 700 أوروبي ذهبوا الي القتال في سوريا بسبب تأثيرهم بوسائل التواصل الاجتماعي.

هذه الامثلة الخجولة التي اخترناها وغيرها من المواد التي تخرج عبر ادوات التواصل الاجتماعي تشكل ظاهرة الارهاب الالكتروني (CYBER TERRORISM)، ولقد تم تصنيف ظاهرة الارهاب الالكتروني على عدة مراحل منها التهديد الالكتروني القصف الالكتروني مثل توجيه مئات الالاف من الرسائل الي مواقع شبكات المعلومات بحيث يضعف قدرتها على استقبال رسائل من المتعاملين معها مايؤدي الي وقف هذا الموقع ، وتدمير أنظمة المعلومات مثل إدخال الفيروسات التي تضر باجهزة الكومبيوتر والمعلومات المخزنة فيها ،والتجسس الالكتروني مثل التلصص وسرقة المعلومات وتتعدد اهداف السرقات وحالات التلصص من معلومات اقتصادية الي سياسية وعسكرية وشخصية .

البعض يقول إن هذه العمليات افتراضية ولايجوز تحميلها اكثر مما يجب،والبعض الأخر يصر على انها عمليات ارهابية حقيقية وليست افتراضية وهي تعرض حياة الاخرين للخطر وتنمي لديهم الشعور بعدم الأمان وبرغبة الانتقام أو مجاراة الشر لرد الإساءة أو اللجوء الى القضاء.

بصراحة لاتوجد منطقة في العالم تحوي او تحتضن اشكال الارهاب مثل المنطقة العربية ولانعلم لماذا تصاب هذه المنطقة بكل الأدران في الوقت الذي استقبلت دول العالم الاخرى نتاج التكنولوجيا – بما فيها وسائل التواصل الاجتماعي – واستخدمته بما يفيد شعو بها وبما يقوي من الرأي العام وينشر حرية التعبير بصورة حضارية لايتدخل فيها التهديد او رفض الاخر او السخرية من الرأي .

وأتذكر أول ماوصل إلينا الهاتف النقال ورسائله النصية فيما بعد ، بدأ كثيرون باستخدام هذه الوسيلة الحضارية في تبادل النكات (السمجة) والرسائل القاتلة للوقت ،وعندما وصلت الينا وسائل التواصل الاجتماعي عبر الانترنت إستحوذ على كثيرين من قاطني هذا العالم العربي (حُبّ) الثأر للذات ومن عدو واضح أو عدو مجهول ؟ وبدأ هذا البعض يقذف العبارات الساخنة والسوداء دون وعي أو انتشاء بوطنية زائفة بحيث تم تلويث الفضاء العربي بتلك الكلمات والمشاهد وصور الانتقامات ورفض الأخر لدرجة أن البعض الصامت أصبح لايدري مع أي لجة يسير تماماً كما حل الاشكال السياسي داخل أروقة وسائل التواصل الاجتماعي وتضاربت الاقوال وضاعت الحقيقة.

نعم نحن نعيش مرحلة إرهاب تكنولوجي وهنالك الكثير من القضايا في المحاكم في الكثير من الدول العربية هذا يعود الي افتقاد ثقافة الحوار والشعور المزيف بـ(الأنا المتضخمة) والفراغ الفكري الذي يجعل من أي شخص – مهما كان مستواه أن يختفي وراء اسم مستعار ويقذف بشخصية سياسية او ادبية او اعلامية دون وجه حق وهذا

بعيد جداً عما يسمونه (حرية التعبير) التي لم استغلها بعض العرب سلبياً بعد ان اخترع لهم الغرب وسائل التواصل الاجتماعي .[58]

جرائم القرصنة:

لقد وفرت شبكة الانترنت في ظل ماتوفره من تقنيات حديثة MODERN TECHNIQUES– لكونها تربط العالم اجمع وتلغى الحدود الجغرافية مما أتاح فرصة ارتكاب الجرائم عابرة الحدود في اوقات قياسية و بأقل قدر من المخاطرة مجالا خصباُ لنمو نوع جديد من أنواع الجرائم لم يكن معروفا في من قبل الا وهو الاستخدام غير المشروع – النسخ الغير مشروع– لنظم تشغيل ولبرامج الحاسب الالي.

وجرائم القرصنة التي تتم عبر شبكة الانترنت لاتقع فقط علي برامج تشغيل الحاسب الالي وانما تقع على اي منتجات فكرية أخرى إذ يتم نسخها .

وتشير التقديرات الي ان هناك حوالي 300 مليار صفحة علي الاقل يتم اعادة انتاجها من خلال الة نسخ واحدة كل سنة على مستوى العالم ويشمل هذا النسخ الصحف والمجلات والنوت الموسيقية .

طبعا هذا الرقم يشمل القرصنة التي تتم مقابل الربح المادي وايضاً القرصنة التي تتم ولكن دون ان يكون هدفها تحقيق الربح المادي فالنسخ للاستخدام الداخلي كالمعاهد والجامعات والمدارس والمؤسسات التعليمية والمستشفيات بشكل عام وحتي المنازل يمكن لهم أن ينسخوا لأغراض داخلية وشخصية .

ولم يعد النسخ هذه الايام مقصوراً على الات التصوير التقليدية فاليوم اصبح النسخ الرقمي الذي يمكن ان يمسح من خلالها ضوئياً ويخزن رقمياً باستخدام النسخ

---

[58] شريهان نشأت المنيري، (مقال) – مجلة الاهرام الالكترونية – دورية متخصصة في الشئون الدولية –عدد الثلاثاء 11 فبراير 2014

عبر الليزر وكذلك الامر بالنسبة لأسلوب النسخ الألكتروستاتيكي الجاف والذي يمكن ان يستوعب (400*600 في كل بوصة) حيث يمكن بعد ذلك بثها في الشبكات وتوسيعها ومسحها ضوئياٍوإعادة طباعتها من خلال كمبيوتر وطابعة عادية وقد تكون في بعض الاحالات الاعمال المنسوخة أفضل نوعية من الاعمال الاصلية.

لقد بات النسخ بدون إذن او ترخيص الي جانب السلبيات والمخاوف التي تخلفها التجارة الالكترونية يزعج ويقلق مالكي البرامج ومنتجيها والناشرين والمؤلفين واصبحت التكنولوجيا المتقدمة ومصدر إزعاج لمالكي الحقوق الفكرية والمعنوية مما دعاهم الي التفكير بتشكيل إدارة جماعية لهذه الحقوق و إحاطة هذه الحماية بأطر قانونية عن طريق المعهدات الدولية لتتمتع بالحماية القانونية من أجل استغلال هذه الحقوق في عقود الترخيص على غرار عقود الترخيص الخاصة باستعمال علامة تجارية أو استغلال براءة اختراع.

ويتذمر مالكو الحقوق الفكرية والمعنوية ليس فقط من القوانين المحلية والقصور في تطبيقها بل حتي من قصور آليات حسم المعاهدات الدولية حيث ان هذه المعاهدات وتلك القوانين كانت قد وضعت عندما كانت الطباعة تتم بالنسخ باليد او بالالة الطابعة العادية وقبل ان يكون هناك الات تصوير ونسخ بالليزر والتي اصبحت تمكن المستعملين والدارسين من حيازة نسخ الكتب والابحاث عن طريق تصويرها ونسخها في المكتبات العامة او الجامعات او المعاهد او المدارس او الشركات لإعادة إنتاج نسخ مجانية لغايات إيضاح التعليم وتسهيله.

هذا من جهة ومن جهة اخرى فأن العولمة التجارية وزيادة استعمال التجاروالمستثمرين الشبكات الدولية والبريد الالكتروني وتبادل رسائل البيانات إلكترونياً وتحويل الكثير من الحكومات الي ما يسمى بالحكومة الالكترونية أدى الي زيادة اهتمام المجتمع الدولي بالضوابط القانونية للتجارة الالكترونية وهذا ماتنبهت له

الجمعية العامة في الأمم المتحدة فوضعت عام 1996م قانوناً نموذجياً للتجارة الالكترونية (لقانون الأونسترال UNCTTRAL LAW) لتقوم الدول الأعضاء بالاسترشاد به[59] .

وقد أدت قرصنة البرامج الي خسائر مادية باهظة جدا وصلت في عام 1988م الي حوالي إحدى عشر مليار دولار امريكي في مجال البرمجيات وحدها ولذلك سعت الشركات المختصة في صناعة البرامج الي الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات و ذلك منظمة اتحاد برمجيات الاعمال او ما يعرف اختصار بـ B S A (BUSINES SOFTWARE ALLIANCE) والتي اجريت دراسة تبين منها ان القرصنة علي الانترنت ستغطى على انواع القرصنة الاخري ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادى القرصنة علي الانترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم علي الانترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج القرصنةالا ان تلك الشركات قد تراجعت عن هذا التهديد أثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الانترنت .

التكييف القانوني للجريمة :

تدخل جرائم القرصنة ضمن نطاق جرائم السرقة وعليه فكل القواعد القانونية التي تنطبق على السرقة تنطبق على جرائم القرصنة .

[59] شبكة الحوار نت الاعلامية – ويكيبيديا الموسوعة الحرة – الشبكة العنكبوتية.

المبحث الثالث : جرائم التجسس الإلكتروني

عمليات التجسس هي عمليات قديمة قدم البشرية وقدم النزاعات البشرية فمنذ تقدم العصور كان الانسان يتجسس على أعدائه لمعرفة اخبارهم والخطط التي يعدونها لمهاجمته ولهذا كان التجسس اهميته الكبيرة علي كافة مستويات النزاعات الانسانية التي مر بها البشر منذ بدء الخليقة .

وقد تطورت عمليات التجسس طبقاً لما يسود المجتمع من تطورات علمية وتكنولوجية. فمثلاً اختراع الرادار ليتجسس على اعدائه ومعرفة كافة تحركاتهم ثم حدث تطور كبير ألا وهو اختراع الاقمار الصناعية التي تقوم بتصوير الانسان والالات الحربية والمدنية والمباني وكل ماهو فوق الأرض يتم تصويره كل فترة زمنية معينة لمعرفة التحركات التي تتم والأن و في ظل التطور التقني الهائل الذي نعيشة فقد أصبح هناك مايعرف بالتجسس الالكتروني .

التجسس الالكتروني (ELECTRONIC ESPIONAGE) لاتكمن خطورته إذا ماكان القائم به هم بعض الهواة العابثين HACKERS وكان الغرض من اختراقهم لأجهزة الحاسبات الالية والشبكات هو العبث بالمحتويات أو إلغاء بعضها أو كلها الان الاهمية تكمن فيما اذا كان القائم بتلك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على الدول الأخرى .[60]

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف اخيراً عن مفتاح وكالة الامن القومي الامريكية (N S A) والتي قامت بزراعته في نظام التشغيل

[60] أسامة الكسواني ، التجسس الالكتروني وطرق مكافحته ، القاهرة : الدار الجامعية ، 2006م ، ص 19.

الشهير ويندوز وربما يكون هذا هو أحد الاساليب الرئيسية التي دعت الحكومة الالمانية باعلانها في الفترة الاخيرة عن استبدالها لنظام التشغيل ونيدوز بأنظمة تشغيل أخرى .

كما كشفت أخيرا النقاب عن شبكة دولية ضخمة للتجسس الالكتروني تعمل تحت إشراف وكالة الأمن القومي الامريكية بالتعاون مع اجهزة الاستخبارات والتجسس في كل من كندا وبريطانيا ونيوزيلندا ويطلق عليها اسم ECHELON أو فاكس أو الكترونياً.

وخصص هذا النظام للتعامل مع الاهداف الغير عسكرية وبطريقة تجعله يتعرض كميات هائلة جداً من الاتصالات والرسائل الالكترونية عشوائياً باستخدام خاصية الكلمة المفتاح بواسطة الحسابات المتعددة والتي تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الاقمار الصناعية الواقعة في منطقة (واى هوباى) بجنوب نيوزيلندا ومحطة (جير الدتون) الموجودة في منطقة (مورينستو) بمقاطعة (كورنوول)في بريطانيا والمحطة الواقعة في الولايات المتحدة الامريكية بمنطقة (شوجر جروف) وتبعد حوالي مائتي وخمسون كيلو مترا جنوب واشنطن وكذلك المحطة الموجودة بولاية واشنطن على بعد مائتي كيلو مترا من جنوب غرب مدينة سياتل.

فمع توسع التجارة الالكترونية عبر شبكة الانترنت تحولت الكثير من مصادر المعلومات الي اهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار الي زيادة نسبة التجسس علي الشركات من 36% عام 1994م الي 45% عام 1999م كما أظهر استفتاء اخر عام 1996م لمسئولي الامن الصناعي في الشركات الامريكية حصول الكثير من الدول وبشكل غير مشروع علي معلومات سرية لانشطة تجارية وصناعية في الولايات المتحدة الامريكية.

ومن الاساليب الحديثة في التجسس الالكتروني إسلوب إخفاء المعلومات داخل المعلومات وهو اسلوب شائع وان كان ليس بالامر السهل ويتلخص هذا الاسلوب في لجوء المجرم الي إخفاء المعلومة الحساسة المستهدفة بداخل معلومة أخري عادية داخل الحاسب الالي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها والغير عادية في داخلها وبلك لا يشك احد في ان هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً فمن الصعب جداًالوصول الي تلك المعلومات المغلقة في في معلومات اخرى غير مشكوك فيها على الاطلاق.

ومن أشهر وأحدث أمثلة التجسس الالكتروني انه بعد الاعتداءات الاخيرة على الولايات المتحدة الامريكية في سبتمبر صدرت تعليمات جديدة لاقمار التجسس الامريكية الصناعية بالتركيز على افغانستان والبحث على اسامة بن لادن والجماعات التابعة والموالية له وقررت السلطات الامريكية الاستعانة في عمليات التجسس على افغانستان بقمرين صناعيين مصممان خصيصاً لالتقاط الاتصالات التي تجرى عبر اجهزة الالسلكي والهواتف المحمولة بالاضافة الي قمرين اخرين يلتقطان سصورا فائقة الدقة وفي نفس الوقت طلب الجيش الامريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لها لرصد الاتصالات ومن ثم تحول بعد ذلك الي الولايات المتحدة الامريكية حيث تدخل في اجهزة كمبيوتر متطورة لتحليلها .

التكييف القانوني للجريمة:

جرائم التجسس جرائم قديمة ومعاقب عليها بأشد العقوبات في كافة القوانين القديمة والحديثة والتجسس الالكتروني هو أحد أشكال التجسس الحديث كالتجسس بواسطة الاقمار الصناعية والتجسس بواسطة طائرات الاستطلاع المتقدمة إلا انه في معظم الاحيان لاتتمكن الدولة رغم علمها بأسم الدولة التي تتجسس عليها من ضبط الشخص الذي سقوم بالتجسس الا في احوال معنية وهى إذا ماكان التجسس يتم

بالشكل القديم والذي يتم بإرسال شخص من الدولة الي الدولة الاخري للحصول على المعلومات من مصادر في تلك الدولة فيتم التمكن من ضبطه .

جريمة تزوير التوقيع الإلكتروني:

بداية عرف القانون المصري لسنة 2004 التوقيع الالكتروني بأنه :(مايوضع على محرر الكتروني ويتخذ شكل حروف او ارقام او رموز او اشارات او غيرها ويكون له طابع متفرد بتحديد شخص الموقع ويميزه عن غيره)).

كذلك عرف ذات القانون المحرر الالكتروني بأنه :(رسالة بيانات تتضمن معلومات تنشأ أو تنشأ او تدمج او تخزن او ترسل او تستقبل كليا او جزيئا بوسيلة الكترونية او ضوئية او بأية وسيلة أخرى مشابهة))، من تلك التعريفات نجد أن التوقيع الالكتروني لايتم برسم شكل كتابي ما بواسطة اليد البشرية وبواسطة قلم أيا كان نوعه جاف أو حبر .... الخ وإنما التوقيع الالكتروني يتم بواسطة منظومة الكترونية تتخذ شكل حروف او ارقام او ايشارات او غيرها بحيث لا يمكن تقليدها وانما يمكن استعمالها دون علم مالكها.

وعليه فتزوير التوقيع الالكتروني يختلف كا الاختلاف عن تزوير التوقيع التقليدي يعني قيام أحد الاشخاص بتقليد توقيع شخص أخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه وذلك لا التوقيع المقلد لايمكن أن بذات خواص التوقيع الخاص بصاحبه وذلك لان التوقيع المقلد لايمكن ان يكون بذات خواص التوقيع الاصلي وبالتالي لايمكن ان يكون متماثل معه .

بينما في جريمة تزوير التوقيع الالكتروني يقوم شخص بسرقة منظومة التوقيع الالكتروني الخاصة بشخص أخر وقيامه باستخدامها في توقيع مستندات الكترونية فهنا نجد ان التوقيع الالكتروني سليم مثله مثلما لو كان مالك منظومة التوقيع قد قام

بالتوقيع بواسطتها وانما المشكلة تكمن هنا ان التوقيع تم بواسطة شخص اخر تحصل على تلك المنظومة عن طريق التجسس الالكتروني او التلصص او ايا كانت الطريقة.

وعليه تكون طريقة الكشف عن التوقيع التقليدي المزور عن طريق مضاهاة التوقيع المزيف بتوقيع الشخص المنسوب اليه هذا التوقيع بينما في حالة تزوير التوقيع الالكتروني لايمكن استخدام تلك الطريقة لاكتشاف تزوير التوقيع إذ انه هنا وكما ذكرنا يكون التوقيع سليم وانما ليس صادراً من الشخص مالك منظومة التوقيع الكتروني فيكون الكشف عن التوقيع الالكتروني المزيف عن طريق إثبات انه ليس صادراً من مالك منظومة التوقيع الالكتروني وتحديد الشخص الذي سرق تلك المنظمة واستخدمها.

وعليه فجريمة تزوير التوقيع التقليدي تختلف اختلاف كلى وجزئي عن جريمة تزوير التوقيع الالكتروني سواء في طريقة التزوير أو في أسلوب اكتشاف هذا التزوير وطرق مكافحته.

وعلى ذلك فقد نص القانون النموذجي الخاص بالتوقيع الالكتروني والصادر من هيئة الامم المتحدة على موثوقية التوقيع الالكتروني وخصصت له عدد من المواد وحددت شروط لابد من توافرها في موثوقية منظومة التوقيع الالكتروني وفي مدى ارتباط تلك المنظمومة المستخدمة بمالكها وقت ان قام باستخدامها لإحداث التوقيع الإلكتروني وذلك ليعتبر توقيعاً إلكترونياً موثوقاً على انه إذا انتفت أي من تلك الشروط أو الاركان التي تم النص عليها في ذلك القانون النموذجي لايعتبر في تلك الحالة توقيعاًإلكترونياً موثقاً.

ومن المعروف أن كافة القوانين الخاصة بالتوقيع الالكتروني والصادرة في كافة دول العالم قد خرجت من تحت عباءة هذا القانون وعليه فإن كافة القواعد والشروط

الخاصة بموثوقية منظومة التوقيع الالكتروني والتي تم النص عليها في هذا القانون النموذجي سنجد انه قد تم النص عليها أيضاً في كافة القوانين الاخري الصادرة في كافة دول العالم.

والموثوقية تم النص عليها ايضا في القانون المصري الخاص بالتوقيع الالكتروني في المواد الرابعة عشر والخامسة عشر إذ تم النص فيهما على ما يلي :-

((المادة الرابعة عشر – للتوقيع الالكتروني في نطاق المعاملات المدنية والتجارية والادارية ذات الحجية المقررة للتوقيعات في احكام قانون الاثبات في المواد المدنية والتجارية إذا روعى في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون)).

((المادة الخامسة عشر – للكتابة الالكترونية وللمحررات الالكترونية وللمحررات الالكترونية في نطاق المعاملات المدنية والتجارية والادارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في احكام قانون الاثبات في المواد المدنية والتجارية متي استوفت الشروط المنصوص عليها في هذا القانون و وفقاً للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون)).

وعليه نجد ان المشروع المصري قد اوقف تمتع التوقيف الالكتروني بالحجية في الاثبات على مراعاة شروط وجود الموثوقية في هذا التوقيع الالكتروني وارتباطه بالموقع دون غيره وهي اعلى درجات الموثوقية في التوقيع الالكتروني .

واما عناصر الموثوقية التي تم النص عليها في القانون المصري فقد تم النص عليها في المادة الثامنة عشر من القانون ففي تلك المادة نص المشروع عن الشروط التي تطلبها في منظومة التوقيع الالكتروني وفي ارتباطها بالموقع وحده دون أي شخص أخر.

أما نص المادة الثامنة عشر فهو كالأتي :-[61]

((يتمتع التوقيع الالكتروني والكتابة الالكترونية والمحررات الالكترونية بالحجية في اثبات إذا ماتوافرت فيها الشروط الاتية:

(أ) ارتباط التوقيع الالكتروني بالموقع وحده دون غيره .

(ب) سيطرة الموقع وحده دون غيره على الوسيط الالكتروني .

(ت) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكترونية أو التوقيع الالكتروني وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك)).

التكييف القانوني للجريمة:

تخضع جريمة تزوير التوقيع الالكتروني بقانون التوقيع الالكتروني الصادر بجمهورية مصر العربية برقم 15 بتاريخ 2004 وقد تم النص فيه على جزاءات لمرتكبي هذا النوع من الجرائم المرتبطة بالتوقيع الالكتروني إذ نصت المادة الثالثة والعشرون من هذا القانون على الأتي :-[62]

((مع عدم الاخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في اي قانون أخر يعاقب باحبس وبغرامة لاتقل عن عشرة الاف جنية ولا تجاوز مائة الف جنية أو بإحدى هاتين العقوبيتين كل من :-[63]

(أ) اصدر شهادة تصديق الكتروني دون الحصول علي ترخيص بمزاولة النشاط من الهيئة .

---

[61] المجلة العربية للدراسات الامنية والتدريب المجلد 28 العدد 56

[62] القانون الصادر بجمهورية مصر العربية برقم 15 بتاريخ 2004

[63] نفس المرجع السابق .

(ب) اتلف او عيب توقيعاً او وسيطاً او محررا الكترونياً او زور شيئاً من ذلك بطريق الاصطناع او التعديل او التحرير او بأي طريق أخر .

(ج) استعمل توقيعاً او وسيطاً او محررا الكترونياً معيباً او مزورا مع علمه بذلك .

(د) خالف ألأي من أحكام المادتين (19) و (21) من هذا القانون .

(هـ) توصل بأي طريقة الي الحصول بغير حق على توقيع او وسيط او محررا الكتروني او اختراق هذا الوسيط او اعترضه او عطله عن أداء وظيفته .

وتكون العقوبة على مخالفة المادة (13) من هذا القانون الغرامة التي لا تقل عن خمسة الاف جنيه ولا تجاوز خمسين ألف جنيه ، وفي حالة العود تزاد العقوبة بمقدار العقوبة المقررة لهذة الجرائم في حديها الأدنى والأقصى.

وفي جميع الاحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار وعلى شبكة المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه .

كما نصت المادة الرابعة والعشرون من ذات لقانون على انه :-[64]

((يعاقب المسئول عن الادارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الافعال التي ترتكب بالمخالفة لأحكام هذا القانون إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الادارة قد أسهم في وقوع الجريمة المنصوص عليها مع علمه بذلك ، ويكون الشخص الاعتباري مسئولا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين به بأسم ولصالح الشخص الاعتباري)).

---

[64] المادة 24 من نفس القانون المذكور في المرجع السابق .

الفصل الثالث

الدليل الإلكترونى

المبحث الاول: الدليل الالكتروني

المعروف ان الادلة الفنية المضبوطة في جرائم نظم المعلومات لها أهمية كبرى وقد يكون فيه الفصل بين الادلة والبراءة للمتهم لذلك ينبغي الاعتناء بتخزين هذه الادلة في بيئة مناسبة حتي لاتفسد .

هنالك أنواع عديدة من الادلة الورقية – مثل مخرجات الطباعة والتقارير والرسوم البيانية. [65]

أ- وادلة أجهزة الحسابات تتضمن معها ملحقات الحاسب في شاشات وغير ذلك .

---

[65] عبدالحافظ عبدالهادي عابد –الاثبات الجنائي بالقرائن-رسالة دكتوراة القاهرة سنة 1989م ص 198

ب- الاقراص المرنه والاقراص العمليه : وهي من اهم الادلة لانها تحتوي على البيانات والمعلومات وكذلك على كلمات المرور والصور والتقارير وعلى خطط ارتكاب الجريمة احياناً .

ت- اشرطة تخزين المعلومات وتستخدم دائماً لحفظ النسخ الاحتياطية.

ث- القطع الالكترونية ومن بين القطع الالكترونية التي يمكن ان تكون لها ادلة مهمة أجهزة الإرسال التي تكون في صورة قطعة الكترونية ولذلك يجب الاهتمام بفحصها للتأكد من طبيعتها خاصة في قضايا التجسس والقرصنة .

ج- أجهزة الموديوم والتي تستخدم في نقل المعلومات ويمتاز بعضها بإمكانية لأن يعمل كجهاز الرد على رسائل الهاتف مما يجعله دليلاً محتملاً بالغ الاهمية .

البرامج وهي تمثل الادوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات.

الطابعات واجهزة تصوير المستندات وماقد تحتويه من اوراق مطبوعة او صورة او ماهو مختزن في ذاكرنها من معلومات .

الأدلة في الجرائم الالكترونية :

اماكن وجود الادلة :على المحقق ان يبحث الادلة في الاماكن المحتمل وجودها وهي الاماكن التالية :- [66]

1-شاشة الحاسب:وهي الموضع المفضل للصق بعض الاوراق اللاصقة الصفراء الصغيرة التي تحمل بعض المعلومات مثل ارقام الهاتف او كلمات المرور .....إلخ.

---

[66] احمد ضياء الدين-مشروعية الدليل في المواد الجنائية رسالة دكتوراة كلية الحقوق جامعة عين شمس عام 1983م ص 473 ومابعدها

2- **بجوار الهاتف:** عادة توجد بجوار الهاتف بعض ارقام الهاتف او الفاكس او بعض الرسائل المختصرة .

3- **حافظة النقود:** تحتوى حافظة النقود عادة بطاقات الإئتمان وبطاقات الهاتف ومذكرات صغيرة وكلمات المرور وربما يوجد قرص مرن في الحافظة .

4- **المفكرة الالكترونية:** بعد إنتشار هذا النوع من المفكرات الالكترونية فهى اصبحت من اهم الادلة التي يجب التحفظ عليها فهي تحتوي على اسماء وارقام هواتف وعناوين بريد الكتروني وغير ذلك من المعلومات الهامة التي قد تكون مفيدة للتحقيق.

5- **جيوب المتهم:** هنالك اقراص مرنة رخيصة تتسع لأكثر من مائة (ميجا بايت) من المعلومات ويمكن ان توضع بسهولة في جيب القميص .

أدوات التحقيق:

أ- برنامج إذن التفتيش Computer Search Warrant Program :

وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الادلة وتسجيل البيانات عنها ، ويجب أن يكون البرنامج جمع المحقق على قرص مرن أو قرص صلب محمول ، ويمكن لهذا البرنامج ان يصدر ايصالات باستلام الادلة والبحث في قوائم الادلة المضبوطة لتحديد مكان دليل معين ،أو ظرف ضبط هذا الدليل . [67]

ب- **قرص بدء تشغيل الحاسب Bootable disk :**

[67] مفهوم الاثبات اوسع من كلمة دليل فالاثبات اكثر عمومية ويشمل مجموعة من الاجراءات الشكلية والموضوعية والقواعد الالزمة لكشف الحقائق

يمكن هذا القرص المحقق من تشغيل الحسابات اذا كان نظام التشغيل فيها محمياً بكلمة مرور وينبغي ان يكون القرص مزوداً ببرنامج مضاعفة المساحة Double Space.

ت- **برنامج معالجة الملفات Xtree pro gold :**

وهو برنامج ممتاز لمعالجة الملفات يمكن بواسطة العثور على الملفات في اي مكان على الشبكة او على القرص الصلب ، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم او الاقراص المرنه المضبوطة ، ويستخدم أيضاً لقراءة البرامج في صورتها الاصلية كما يمكن استخدامه للبحث عن كلمات معينة او عن اسماء ملفات او غير ذلك .

ث- برنامج Lap Link :

يفيد للحصول على نسخة من المعلومات قبل اي محاولة لتدميرها من جانب المتهم.

ج- برنامج كشف الفيروسات وتدميرها :

فهو لضمان حماية جهاز الحاسب الخاص بالمحقق .

ح- برنامج Ana Disk \ View Disk :

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كان اسلوب تهيئته.

خ- برنامج الدمج وفك الدمج pkzip :

ويستخدم لفك دمج البرامج فربما كان المتهم قد قام بدمج برامجه – وفي هذه الحالة لايمكن الاطلاع عليها إلا بعد فك الدمج .

وهنالك ادوات ينبغي ان تكون حاضرة مثل مجموعة كاملة من المفكات والمفاتيح وجهاز لنسخ المعلومات الى قرص صلب .

فحص مسرح الجريمة:

يبدأ ذلك بمعاينة الموقع لمعرفة الداخل والمخارج ثم يتم تكوين فريق المداهمة مع وضع خطة المداهمة بعد استخراج اذن التفتيش بعد المداهمة وقبل المغادرة يجب الاهتمام بمراجعة أخيره للفرق .

وبعد توثيق العملية وتسجيل الدروس المستفادة للاستفادة .

ماهية الدليل الرقمي "الالكتروني" وأقسامه وخصائصه:

ترتكز عملية الاثبات الجنائي للجرائم الرقمية على الدليل الجنائي الرقمي باعتباره الوسيلة الوحيدة والرئيسية لاثبات هذه الجرائم وهو محور اهتمام بحثنا هذا لذا سنتناول توضيح ماهية هذا الدليل وخصائصه واقسامه حيث نوضح فيه مفهوم الدليل الجنائي بشكل عام .

الدليل في اللغة :

هو المرشد ومايتم به الإرشاد ومايستدل به والدليل : الدال ، والجمع : أدلة[68] وكذلك يعني تأكيد الحق بالبينة ، والبينة هي الدليل أو الحجة .

الدليل في المصطلح القانوني :

يقصد بالدليل : الوسيلة التي يستعين بها القاضي للوصول الي الحقيقة التي ينشدها ، والمقصود بالحقيقة في هذا الصدد :

هو كل ما يتعلق بالاجراءات والوقائع المعروضة عليه حكم القانون عليهاكما يقد بالدليل او العمل الاجرائي :كل إظهار لنشاط عام او خاص داخل الخصومة او من اجلها يؤدي مباشرة الي التأثير في تطوير رابطة الخصومة او بمعني أخر :هو كل

[68] جميل صليبا- المعجم الفلسفي- بيروت-دار الكتاب اللبناني-الطبعة الاولي سنة 1970م ص23

عمل يجري في الخصومة اويهدف الي اعدادها او له قيمة في الخصومة ، اياً كانت طبيعته او معناه ، نظمه القانون بقصد الوصول الي تطبيق القانون الموضوعي فيه، وهوالوسيلة الاثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن اليها وهو أداة الإثبات عموماً . [69]

كما أن الدليل هو : الوسيلة المتحصلة بالطرق المشروعة لتقديمها للقاضي لتحقيق اليقين لديه والحكم بموجبها[70] .

والدليل هو النشاط الاجرائي الحال والمباشر من أجل الحصول على اليقين القضائي وفقاً لمبدأ الحقيقة المادية وذلك عن طريق بحث أو تأكيد الاتهام أو نفيه [71]

تعريف الدليل الالكتروني الجنائي:

يمكن لنا أن نعرف الدليل الالكتروني الجنائي باعتباره نوعاً متميزاً من أنواع الدليل الجنائي.

الدليل الجنائي بأنه " الدليل المأخوذ من أجهزة الحاسب الالي ويكون فيعرف البعض

في شكل مجالات او نبضات مغناطيسية او كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء".[72]

---

[69] ناصر ابراهيم محمد زكي-سلطة القاض الجنائي في تقدير الادلة جامعة الازهر كلية الشريعة والقانون 1987م ص211.
[70] محمد عبيد سعيد سيف مشروعية الدليل في المجالين الجنائي والتأديبي دراسة مقارنة –رسالة دكتوراة في علوم الشرطة –مصر- ص 136
[71] احمد ضياء الدين محمد خليل-قواعد الاجراءات الجنائية ومبادئها في القانون المصري –مطبعة كلية الشرطة سنة 2004م ص
[72] ممدوح عبدالحميد عبدالمطلب-البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الالي والانترنت –مرجع سابق ص 88

وهو مكون رقمي لتقديم معلومات في أشكمال متنوعة مثل :النصوص المكتوبة أوالصور والاصوات والاشكال والرسوم وذلك من اجل الرباط بين الجريمة والمجرم والمجنى عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون.

أو هو " معلومات يقبلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية[73]

وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الالي وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شئ أو شخص له علاقة بجريمة أو جانى أو مجني عليه .

في حين عرفه البعض الاخر بأنه " الدليل الذي يجد له أساس في العالم الافتراضي ويقود الي الجريمة.[74]

ويقدم بحثين أخرين تعريفاً للدليل بأنه :" هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية ، وأجهزة ومعدات وأدوات الحاسب الالي ، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة اورسومات أو صور وأشكال وأصوات ،لإثبات وقوع الجريمة ولتقرير البراءاة أو الادانة فيها ".

تقسيمات الدليل الالكتروني الجنائي:

تختلف الجريمة المعلوماتية عن الجريمة التقليدية في كون الأولى تتم في بيئة مادية عبر نظام حاسب ألي ، أو شبكة المعلومات الدولية الانترنت حيث يمكن

---

[73] اللواء د.محمد الامين البشري-التحقيق في الجرائم المستخدمة-الطبعة الاولي-جامعة نايف العربية للعلوم الامنية الرياض سنة 2004م ص 234

[74] د.عمر محمد بن يونس-مذكرات في الاثبات الجنائي عبر الانترنت ندوة الدليل الرقمي

للجاني عن طريق (نبضات الترونية رقمية) لا ترى أن يبعث في بيانات الحاسب أو برامجه وذلك في وقت قياسي قد يكون جزءاً من الثانية ، كما يمكن محوها في زمن قياسي كذلك قبل أن تصل يد العداله اليه ،مما يحصل الحصول على دليل مادى في مثل هذه الجرائم ،حيث تغلب الطبيعة الالكتروني على الدليل المتوافر [75]

كما أن الدليل الرقمي ليس صورة واحدة بل يوجد له العديد من الصور والأشكال وقد قسمها البعض الي الأقسام الرئيسية التالية:-[76]

1-أدلة رقمية خاصة بأجهزة الحاسب الالي وشبكاتها .

2-أدلة رقمية خاصة باشبكة العالمية للمعلومات الانترنت .

3-أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

4- أدلة خاصة بالشبكة العلمية للمعلومات .

وهذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسب الالي و وفقاً لما قررته وزارة العدل الامريكية سنة 2002م فأن الدليل الرقمي يمكن تقسيمه إلى ثلاث مجموعات وهي كالتالي :-

خ-السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت

---

[75] لواء د.نبيل عبدالمنعم جاد- جرائم الحاسب الالي-بحث منشور بندورة المواجهة الامنية للجرائم المعلوماتية مركز دعم اتخاذ القرارباقيادة العامة لشرطة دبي مطبعة بن دسمال –دبي سنة 2005م ص 128

[76] انظر د:ممدوح عبدالحميد عبدالمطلب-البحث والتحقيق الجنائي الرقمي في جرائم الحاسوب الالي والانترنت –مرجع سابق ص 88

د- السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبرمخرجات برامج الحاسوب وبالتالي لم يسلمها الانسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الالي ATM.

ذ- السجلات التي جزء منها تم حفظه بالادخال وجزء أخر تم إنشاؤه بواسطة الحاسوب ومن الامثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها الي برامج اوراق العمل مثل Excel ومن ثم تمت معالجتها من خلال البرانامج بإجراء العمليات الحسابية عليها ويلاحظ أن التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه ، وإنما تعدد وسائل التوصيل اليه ، و في كل الاحوال يظل الدليل المستند منه رقمياً حتى زأن اتخذ هيئة أخري ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الاخري يكون مؤسساً علي طابع افتراضي مبناه أهمية الدليل الرقمي ذاته وضرورته إلا انه لكي يحدث تواصل بين القانون وبين الدليل المذكور نتيجة لنفص توافر الامكانيات الرقمية في المحاكم فإنه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلاً أصلياً.

خصائص الدليل الالكتروني الجنائي:

يتميز الدليل الالكتروني عن الدليل التقليدي بالخصائص التالية :-[77]

أ- الادلة الرقمية تتكون من بيانات ومعلومات ذات هئية الكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب أدركها الاستعاة بأجهزة ومعدات الحسابات الالية Hardware واستخدام نظم برنامجية حاسوبية Software .

ب- الادلة الرقمية ليست أقل مادية من الدليل المادي فحسب بل تصل الى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن[78] وذلك لأن مصطلح

---

[77] د.عمر محمد بن يونس-مذكرات في الاثبات الجنائي عبر الانترنت – ندوة الدليل الرقمي –مرجع سابق- ص 12

[78] محمد الامين البشري-التحقيق في الجرائم المستحدثة-مرجع سابق – ص 237 ومابعده

الدليل الرقمي يشمل كافة أشكال وانواع البيانات الرقمية الممكن تداولها رقمياً بحيث يكون بينها وبين الجريمة رابطة من نوع ما وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني .

ت- يمكن استخراج نسخ من الادلة الجنائية الرقمية المطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشئ الذي لايتوافر في أنواع الادلة الاخري التقليدية مما يشكل ضمانه شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق عمل نسخ أخري طبق الاصل من الدليل مما حذا بالمشروع البلجيكي تم بمقتضي قانون 28 نوفمبر 2000م تعديل قانون التحقيق الجنائي تم بإضافة المادة 39 bisالتي سمحت بضبط الادلة الرقمية مثل :نسخ المواد المخزنة في نظم المعالجة الالية للبيانات بقصد عرضها على الجهات القضائية.

ث- الادلة الرقمية يمكن يمكن استرجاعها بعد محوها ، واصلاحها بعد إتلافها واظهارها بعد إخفائها ممايؤدي الي صعوبة الخلاص منها وهي خاصية من أهم خصائص الدليل الرقمي بالمقارنة بالدليل التقليدي فهناك العديد من البرامج الحاسوبية التي وظيفيتها أستعادة البيانات التي تم حذفها أو إلغاؤها سواء تم ذلك بالامر delete وحتي لو تم عمل إعادة تهيئة أو تشكيل للقرص الصلب disK Hard باستخدام الامر Foramt والبرامج التي تم إتلافها أو إخفائها سواء كانت صوراً أو رسوماً أو كتابات أو غيرها. ممايعني صعوبة إخفاء الجاني لجريمته او التخفي منها عن أعين الأمن والعدالة طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة .

ج-الادلة الجنائية الرقمية ذات ديناميكية فائقة السرعة تنتقل من مكان لأخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان ويمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد ، كما أنه يسجل عاداته وسلوكياته وبعض الامور

الشخصية عنه ، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي . [79]

أهمية الدليل الالكتروني الجنائي:

للدليل الالكتروني اهمية كبرى ودور اساسي في معرفة كيفية حدوث الجريمة ولتأكيد ذلك لابد وان يحتوى التطبيق الجنائي على هذا الدليل ويجب ان تكون المنشأة على استعداد وتأهب لمثل هذه الامور غير الاعتيادية ، ويجب ان يكون الاشخاص المسئولون عن التعامل مع هذه الامور على فهم كبير واضطلاع بالامور التقنية والاعيبها وكيفية التعامل بها . [80]

المبحث الثانـــي : قواعد الإثبـات الالكتروني

أهمية قواعد الاثبات الالكتروني:

تمثل قواعد الاثبات أهمية خاصة إذ أن الحق في موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند اليها ، فالدليل هو عصب الواقعة[81] أو هو النتيجة التي تحققت باستعمال وسائل الاثبات المختلفة أي إنتاج الدليل[82].

يقصد بهذا الاثبات : القواعد المتعلقة بالحث عن الادلة وإقامتها أمام القضاء وتقديرها من جانبه[83] فالاثبات هو مجموع الاسباب المنتجة لليقين وبالتالي فإن الاثبات في المواد الجنائية ماهو إلا كافة الادلة التي تؤكد وقوع الجريمة ونحقق حالة اليقين لدى القاضي لإدانة المتهم ، أو ترجح حالة الشك لديه فيقضي بالبراءة ، أو هو كل مايؤدي الي إظهار الحقيقة ولأجل الحكم على المتهم في المسائل الجنائية يجب إثبات

---

[79] ممدوح عبدالحميد عبدالمطلب- استخدام برتوكول في بحث وتحقيق الجرائم على الكمبيوتر ،المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الالكترونية منظم المؤتمر اكاديمية شركة دبي مركز البحوث والدراسات رقم العدد 4 المحور الامني والاداري تاريخ الانعقاد 26ابريل 2003م دبي الامارات العربية المتحدة ص 649-650

[80] عمر محمد بن يونس-مذكرات في الاثبات الجنائي عبر الانترنت ندوة الدليل الرقمي- مرجع سابق- ص 12

[81] احمد ضياء الدين –مشروعية الدليل في المواد الجنائية –مرجع سالق- ص 359 ومابعده

[82] رفعت عبدالفتاح حلاوة –الاثبات الجنائي قواعده وادلته –دار النهضة العربية –القاهرة سنة 2003م ص 19

[83] محمد زكي ابو عامر- الاثبات في المواد الجنائية- الفنية للطباعة والنشر –الاسكندرية- سنة 1985م ص 19

وقوع الجريمة في ذاتها وأن المتهم هو المرتكب لها أو بعبارة أخري وقوع الجريمة بوجه عام ونسبتها للمتهم بوجه خاص.[84]

وحتي يتحقق الدليل اللازم للإثبات فإنه لابد من جمع عناصر التحقيق والدعوى وتقديم هذه العناصر الي سلطة التحقيق الابتدائي فإن أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المهتم قدمته الي المحكمة ومرحلة المحكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة المتهم وإلاقضى ببراءته [85].

إن التطور التقني في شبكة الانترنت سوف يقود دون شك تغيير كبير ، إن لم يكن كلياً في المفاهيم السائدة حول الدليل ، ويقود مثل هذا القول في الحقيقة الي إعلان أنضمام الخبرة التقنية الي علم الخبرة المتميزة بتصنيف التعامل مع موضوع الدعوى من حيث ضرورة الاستعانة بالمختصين في مجال النزاع.

ويعد كل من المعاينة والتفتيش والشهادة أحد وسائل جمع الادلة ولكل منها قواعد يتم إتباعها :- [86]

المعايـنـة :

يرى البعض ان المعاية تتضائل في الجريمة المعلوماتية وذلك لندره تخلف أثار مادية عند ارتكاب الجريمة المعلوماتية ، كما ان طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الاثار عنها بسبب العبث او المحو او التلف لتك الاثار.

---

[84] على زكي العرابي- المبادئ الاساسية للتحقيقات والاجراءات الجنائية- طبعه لجنة التليف والترجمة سنة 1940 ص5

[85] محمود مصطفى ، الاثبات في المواد الجنائية في القانون المقارن –الجزء الاول- النظرية العامة الطبعة الاولى - جامعة القاهرة 1978 ص 3

[86] هاشم فريد رستم – الجوانب الاجرائية للجرائم المعلوماتية-دراسة مقارنة –مكتبة الالات الحديثة اسيوط- مصر 1994م-ص 141 ومابعدها

وعند أجراء المعاينة بعد وقوع الجريمة في المجال الالكتروني فيجب مراعاة الضوابط التالي:-[87]

أ- تصوير الحاسب والاجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة .

ب- احضار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتي يستعيد من الناحية الفنية والعملية .

ت- اعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل

ث- العناية بالطريقة التي تم بها اعداد النظام .

ج-ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتي يمكن اجراء عمليات المقارنة والتحليل حين علرض الامر فيما بعد على المحكمة.

ح-عدم نقل أي ماده معلوماتية من مسرح الجريمة قبل اجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أيث مجال لقوي مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة .

خ-التحفظ على معلومات سله المهملات من الاوراق الملقاة أو الممزقة و أوراق الكربون المستعملةوالشرائط والاقراص الممغنطة غير السليمة ، وفحصها وترفع من عليها البصمات ذات الصلة بالجريمة .

د- التحفظ علي مستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة .

ذ- قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

---

[87] هاشم فريد رستم – الجوانب الاجرائية للجرائم المعلوماتية–مكتبة الالات الحديثة اسيوط- مصر 1994م-ص 59

ر-أن تتم الاجراءات وفق مبدأ المشروعية وفي اطار ماتنص عليه القوانين الجنائية والمعاينة وان كانت واردة في كل الجرائم الا ان أهميتها تتضاءل في بعض بعض الجرائم مثل جريمة الفعل المعنوي وجريمة السب فأن المعاينة فيها غير ذات جدوى اما معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة فيها فيكون ذا أهمية متمثلاً في تصوير كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفر الادلة المادية التي يمكن تجميعها عن طريق هذه المعاينة لكم هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الاشياء التي قد تفيد في إثبات وقوعها ونسبتها الي مرتكبيها.

التفتيش :

ماهية التفتيش في الجرائم المعلوماتية:

إن لكل فرد من أفراد المجتمع الحق في التمسك بحق سرية حياته الخاصة وحماية هذا الحق من الانتهاك سواء أكانت هذه السرية تتمثل في شخصه أو مسكنه أو مراسلاته أو معلوماته المخزنة في حاسوبه أو نظامه المعلوماتى، وله الحق في التمتع بحماية القانون لهذا الحق وهو من الحقوق الدستورية للمواطن التي لا يجوز انتهاكها دون مبرر قانوني، وعلى هذا الأساس يتطلب في بعض الأحيان انتهاك هذا الحق وكشف هذه السرية في سبيل الوصول إلى الحقيقة التي ينشدها القانون وهذا الخرق يكون بموجب إجراء ينص عليه القانون وهو التفتيش.

إن التفتيش إجراء قانوني يمس بحرية الأشخاص وحرمة مساكنهم، وله صور عديدة، كالتفتيش القضائي، الإداري، الوقائي، الاستثنائي، إلا أن ما يهمنا هنا هو التفتيش القضائي الذي يتم إجراؤه بإذن قضائي وبالاستناد إلى القانون، وللتفتيش خصائص مميزة، هي: الجبر، المساس بحق السر، ويهدف إلى الحصول على الأدلة التي تساعد في كشف الحقيقة في جريمة جار التحقيق فيها سواء كانت هذه الأدلة

مادية أو أدلة إلكترونية، وهذا يعنى أن التفتيش ليس بدليل بحد ذاته وإنما هو وسيلة للحصول على الدليل. [88]

شروط التفتيش في الجرائم المعلوماتية:

لما كان التفتيش من الإجراءات الخطيرة التي تمس الحرية الشخصية، وتنتهك مستودع سر الإنسان وراحته وهدوئه كان لا بد أن يتم وضع قيود وضوابط لتنظيم التفتيش لكي يكون هذا الانتهاك لحرية الإنسان قانونياً ووفق ضوابط محددة، لضمان عدم التجاوز على حرية الإنسان إلا وفقاً لما هو ضروري لمصلحة التحقيق إذ أن التفتيش إجراء من إجراءات التحقيق يمثل تغليباً لمصلحة المجتمع على مصلحة الأفراد غير أن تغليب مصلحة المجتمع لا يعنى التعسف في انتهاك حرية الأشخاص وانتهاك حرمة منازلهم ومستودع أسرارهم وعلى هذا الأساس وضع المشرع قيوداً وضوابط تضمن عدم التجاوز على حرية الأشخاص وحرمة منازلهم إلا في إطار حاجة التحقيق.

وهناك نوعان من الشروط التي يستلزم توافرها لضمان صحة التفتيش وهى الشروط الموضوعية والمتعلقة بسبب التفتيش ومحل التفتيش، والجهة القائمة به ، وهناك الشروط الشكلية وتتعلق بالإجراءات المتعلقة بكيفية إجراء التفتيش، كالإذن ووقت إجراء التفتيش وتنظيم المحضر ، أما التفتيش في الجرائم المعلوماتية العابرة للحدود أي التفتيش الذي يتم بحثاً عن أدلة معلوماتية مخزنة في نهايات طرفية تقع خارج حدود الدولة، فله ضوابط خاصة وذلك كما يلي: [89]

الشروط الموضوعية:

[88] العبيدي اسامة بن غانم ، التفتيش عن الدليل في الجرائم الالكترونية – المجلة العربية للدراسات الامنية المجلد29 العدد 58 نوفمبر-ديسمبر 2013

[89] على حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت ط1 عالم الكتاب الحديث، اربد، ص62

لإجراء التفتيش في الجرائم المعلوماتية لابد من وجود سبب للتفتيش، ومحل للتفتيش، و الجهة التي تباشر التفتيش، وذلك كما يلي:

سبب التفتيش:

المقصود بسبب التفتيش، الدافع أو المبرر المقتضى لإجرائه، ويتحقق هذا السبب بوقوع جريمة معلوماتية، واتهام أشخاص معينين بارتكاب جريمة معلوماتية أو الاشتراك فيها، ووجود دلائل قوية على وجود محل الجريمة في المكان أو لدى الشخص المراد تفتيشه، ووجود غاية معينة من وراء إجرائه.

وقوع جريمة معلوماتية:

يشترط لإجراء التفتيش أن تكون الجريمة قد وقعت بالفعل، فلا يجوز إجراء التفتيش بحثاً عن أدلة جريمة مستقبلية ولو كان هناك احتمال في أنها سوف تقع ، والسبب في ذلك هو أن التفتيش من الإجراءات الخطيرة التي تمس حرية الأشخاص وحرمة حياتهم، فلا يجوز انتهاكها إلا إذا ارتكبت جريمة بالفعل فلا يجوز بمجرد وجود احتمال ارتكاب جريمة أن يتم انتهاك حرية الأشخاص ومنازلهم. ولقد نص المشرع العراقي على أنه لا يجوز تفتيش الأشخاص أو الأماكن إلا إذا كان الشخص متهماً بارتكاب جريمة، ولم يحدد المشرع العراقي نوع الجريمة المرتكبة ويعنى ذلك أن التفتيش جائز في جميع أنواع الجرائم، الجنايات، الجنح، والمخالفات كما ورد في المادة 75 من قانون أصول المحاكمات الجزائية العراقي. ومن التشريعات التي نهجت نفس نهج المشرع العراقي، قانون الإجراءات الجنائية الإيطالي الذي أجاز إجراء التفتيش بالنسبة لجميع الجرائم سواء أكانت جنايات أو جنح أو مخالفات.

إن موقف المشرع العراقي حول إجازته التفتيش في جميع أنواع الجرائم محل نظر، ذلك لأن جرائم المخالفات من الجرائم البسيطة التي تكون عقوبتها إما الغرامة

أو الحبس البسيط وهذا يدل على أنها جرائم غير جسيمة، لذلك فإن إجازة إجراء التفتيش وهو من الإجراءات الخطيرة الماسة بحرية الأشخاص وحرمة منازلهم لا تتناسب مع بساطة تلك الجرائم، أما المشرع المصري فقد غاير موقف المشرع العراقي، إذ لم يجز إجراء تفتيش المنازل إلا في جرائم الجنايات والجنح، وهذا الموقف نابع من حرصه وتقديره لخطورة هذا الإجراء، والذي يمس حرية الأشخاص وحرمة منازلهم لذلك فقد حصرها في الجنايات والجنح فقط دون المخالفات لضآلة أهميتها[90] . وقد ساير قانون الإجراءات الجنائية القطري نفس موقف المشرع المصري إذ لم يجز إجراء تفتيش المنازل إلا في الجنايات والجنح.

ولقد عالجت العديد من تشريعات الدول هذه الجرائم، وذلك بإصدار تشريعات تتصدى لهذه الجرائم وتعاقب مرتكبيها، ففي بريطانيا صدر قانون إساءة استخدام الحاسوب 1990 الذي عالج في نصوصه الجرائم المرتكبة بواسطة الحاسوب ومن هذه الجرائم، جريمة الدخول غير المصرح به إلى الحاسوب وجريمة تعديل بيانات الحاسوب كما ورد في Computer misuse act 1990 .

أما في الولايات المتحدة فقد صدر قانون الاحتيال وإساءة استخدام الحاسب سنة 1986، وصدرت قوانين على مستوى الولايات الأمريكية، ومن هذه القوانين، قانون جرائم الحاسوب لولاية فرجينيا عام 1984 (Virginia state computer crime act 1984)، وقانون جرائم الحاسوب لولاية أيوا الصادر عام 1989 (Iowa state computer crime act 1989).

وعالجت هذه القوانين الجرائم المعلوماتية، ولقد لحقت بعض الدول بركب الدول التي سبقتها في معالجة الجرائم المعلوماتية وإصدار التشريعات الملائمة لها، ففي الإمارات صدر قانون مكافحة تقنية المعلومات عام 2006 والتي عالجت هذه

---

[90] فرج علواني هليل، التحقيق الجنائي والتصرف فيه والادلة الجنائية، دار المطبوعات الجامعية ، الاسكندرية 2006، ص 592

الجرائم ومنها، الدخول غير المصرح به إلى نظام معلوماتي، والتزوير المعلوماتى، تعطيل أو إعاقة الوصول إلى الخدمة أو الأجهزة والبرامج كما ورد في المواد 2،3،4،5،6 من قانون مكافحة تقنية المعلومات، بدولة الإمارات العربية المتحدة.

وأصدرت المملكة العربية السعودية عام 2007 م نظام مكافحة جرائم المعلوماتية السعودي والذي عالج الجرائم المعلوماتية، ومنها الدخول غير المصرح به إلى نظام معالجة البيانات، والتزوير المعلوماتى، وتعطيل الشبكات وتدمير البيانات وإتلافها وغيرها من الجرائم كما في المادتين 5،6 من نظام مكافحة جرائم المعلوماتية السعودي.

إذن تفتيش نظم الحاسوب:

إن الحصول على إذن القاضي لتفتيش نظم الحاسوب يعتمد على المكان الذي يوجد فيه الحاسوب، إذ قد يوجد الحاسوب بحوزة شخص معين يحمله معه كجهاز الحاسوب المحمول (لاب توب)، أو قد يكون الحاسوب موجوداً داخل سيارة وكما يلي:-

أولاً: وجود جهاز الحاسوب بحوزة الشخص:

إذا كان محل الجريمة المعلوماتية وهو جهاز الحاسوب وما يحويه من بيانات معلوماتية بحوزة شخص معين كأن يكون جهاز حاسوب متنقل (لاب توب)، وفى هذه الحالة تطبق القواعد القانونية الخاصة بإذن تفتيش الأشخاص، ففي العراق لا يجيز قانون أصول المحاكمات الجزائية العراقي تفتيش أي شخص إلا بناءً على أمر

صادر من سلطة مختصة قانوناً كما ورد في نص المادة 73 أ من قانون أول المحاكمات الجزائية العراقي، ومنح القانون الصلاحية لقاضى التحقيق لتفتيش أي شخص إذا كان متهماً بارتكاب جريمة وكان من المحتمل أن يسفر التفتيش عن وجود أوراق أو أسلحة أو آلات أو وجود أشخاص اشتركوا في الجريمة أو حجزوا بغير حق، ويتضح مما تقدم أن قانون أصول المحاكمات الجزائية العراقي لا يجيز تفتيش الأشخاص إلا بإذن من قاضى التحقيق، لما لهذا الإجراء من مساس بحرية الشخص، إلا أن القانون أجاز للقائم بالتفتيش أن يقوم بتفتيش أي شخص موجود في المكان المراد تفتيشه إذا اشتبه في أنه يخفى شيئاً يجرى من أجله التفتيش، ومعنى ذلك أن القائم بالتفتيش يستمد إذن تفتيش الشخص في المكان من الإذن الخاص بتفتيش المكان الذي حل عليه من قاضى التحقيق[91] ،أما تفتيش المقبوض عليه فهو إجراء يقوم به من قبض عليه لتجريده من أي سلاح قد يحمله ومن المحتمل أن يؤذى به من قبض عليه، وقد يكون حائز جهاز الحاسوب هو المتهم أو أي شخص أخر كمشغل الحاسوب أو المبرمج وغيرهم، وفى هذه الحالة يجوز تفتيشهم أيضاَ إذا أشتبه فيهم من قبل القائم بالتفتيش بأنهم يخفون جهاز الحاسوب المحمول الذي قد يكوم صغير الحجم إلى درجة يمكن إخفاؤه في الملابس.

وأجاز قانون الإجراءات الجنائية القطري لمأمور الضبط القضائي في الأحوال التي يجوز فيها القبض على المتهم أن يفتشه للبحث عما يكون بجسمه أو ملابسه أو ما يحمله من أمتعة أو أشياء تتعلق بالجريمة الجاري التفتيش بشأنها كما ورد في المادة 47 من قانون الإجراءات الجنائية القطري، كما أجاز لمأمور الضبط القضائي وفى حالة وجود قرائن ضد المتهم أو ضد شخص موجود في المنزل الذي يتولى تفتيشه أنه يخفى معه شيئاً يفيد في كشف الحقيقة أن يفتشه كما ورد في المادة 52

---

[91] شرح قانون أصول المحاكمات الجزائية،ط1،دار الحامد،الأردن،2009، ص 106

من قانون الإجراءات الجنائية القطري، ولا يجوز لعضو النيابة العامة الذي يتولى تفتيش المتهم أن يفتش غيره إلا إذا أتضح من إمارات قوية انه حائز لأشياء تفيد الجريمة كما ورد في المادة 75 من قانون الإجراءات الجنائية القطري. أن تفتيش الأشخاص في قانون الإجراءات الجنائية القطري سواءً كان من قبل عضو النيابة العامة أو مأمور الضبط القضائي لا يجوز إلا فى حالة صدور أذن كتابي من النيابة العامة بتفتيش المنزل الموجود فيه المتهم أو الشخص إذ يمتد أمر التفتيش إليهم إذا أعتقد عضو الضبط القضائي أو عضو النيابة العامة أنهم يخفون أشياء تفيد الجريمة أو في حالة القبض القانوني على المتهم.

وأجاز قانون الإجراءات الجنائية الكرواتي تفتيش الأشخاص بحثاً عن الأشياء ومحل الجريمة ويشمل التفتيش ملابس الشخص وكل ما يحمله من منقولات، وإذا كان الشخص معوقاً وتم تركيب أطراف اصطناعية له يتم نزع هذه الأطراف وتفتيشها، ويصدر أمر تفتيش الأشخاص من قبل قاضى التحقيق. وأجاز قانون الإجراءات الجنائية الفيدرالي الأمريكي تفتيش الأشخاص بأذن من قاضى التحقيق.

من خلال استعراض النصوص القانونية السالفة الذكر نستنتج أن تفتيش الأشخاص يجب أن يكون بناءً على إذن من السلطة المختصة بذلك مع الإشارة إلى أن غالبية التشريعات اتفقت على وجوب تفتيش الأنثى من قبل الأنثى مراعاةً للقيم والعادات

(ومن هذه التشريعات، العراقي، المصري، القطري، الكرواتي).

ثانياً: وجود جهاز الحاسوب في مسكن:

المسكن هو المكان الذي يلجأ إليه الإنسان ويتخذه مقراً له سواء كان ذاك بصورة دائمة أو مؤقتة، والمسكن يشمل المكان المسكون فعلاً أو المعد للسكن

كالبيت في القرية والذي يرتاده الشخص بين فترة وأخرى ويشمل هذا المسكن ملحقاته كالكراج، حظيرة الحيوانات، الحديقة، المخزن، أو أى ملحق أخر ضمن حدود المسكن، والمسكن هو مستودع سر الإنسان لا يجوز تفتيشه إلا فى الأحوال التي قررها القانون ، ويخضع المسكن لحماية القانون بغض النظر عن شكله أو هيئته فقد يكون المسكن مبنياً من الكونكريت أو من الخشب أو حتى خيمة أو عربة أو يخت....الخ، ولا يهم أن يكون الشخص الساكن فيه مالكاً له أو مستأجرا كبيت الإيجار أو غرفة الفندق......الخ [92]

المهم أن يكون تحت حيازته ، وعرفت محكمة النقض المصرية المنزل بأنه (المكان الذي يقيم فيه الشخص بصفة دائمة أو مؤقتة أو هو المكان الذي يتخذه الشخص سكناً له على وجه التوقيت أو الدوام بحيث يكون حرماً أمناً لا يباح لغيره دخوله إلا بإذن) [93]

فإذا كان جهاز الحاسوب المراد تفتيشه موجوداً في مسكن معين سواء أكان هذا المسكن عائداً للمتهم أو لأي شخص أخر غيره، فانه يجب أولاً الحصول على إذن قضائي بتفتيش المسكن الذي يوجد فيه جهاز الحاسوب، ولا يحتاج بعد الحصول على إذن لتفتيش المسكن الحصول على إذن أخر لتفتيش جهاز الحاسوب الموجود فيه وذلك لأن إذن التفتيش الخاص بالمسكن يمتد إلى الأشخاص والأشياء الموجودة في هذا المسكن.

أما إذا كان جهاز الحاسوب المراد تفتيشه موجوداً في مكان أخر غير المسكن كالمحلات الخاصة مثل المكاتب التجارية، مكاتب المحامين، عيادات الأطباء أو المحلات العامة كالسينما، والملاهي، ومقاهي الانترنت وغيرها من المحلات العامة،

---

[92] النظرية العامة للتفتيش، ط1، دار النهضة العربية، القاهرة، 1972، ص 231،

[93] التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، ط1، دار الثقافة، عمان، 2008، ص44

فان التفتيش القضائي لهذه الأماكن لا يجوز أيضاً إلا بإذن من السلطة المختصة بإصداره كما ورد في كتاب شرح قانون أصول المحاكمات الجزائية [94]

وقد كان قانون أصول المحاكمات الجزائية العراقي صريحاً في ذلك عندما لم يسمح بتفتيش منزل المتهم أو أي مكان أخر تحت حيازته دون إذن أو إذا كان المكان يعود لشخص أخر غير المتهم كما ورد في المادتين 75،76 من قانون أصول المحاكمات الجزائية العراقي، أما قانون الإجراءات الجنائية المصري فنص هو الأخر على جواز تفتيش أي مكان ولكن بإذن من قاضى التحقيق كما ورد في المادة (91) ف 2 من قانون الإجراءات الجنائية المصري، أما بخصوص تفتيش السيارات فإنه يجوز تفتيش السيارة التي تحت حيازة الشخص أو داخل كراج مسكنه، ويجوز تفتيش السيارة متى ما تم الحصول على إذن بتفتيش الشخص أو مسكنه لان القائم بالتفتيش يستمد إذن تفتيش السيارة من إذن تفتيش الشخص أو المسكن .[95]

أما إذا كانت السيارة واقفة في الطريق العام فإن تفتيشها جائز دون إذن إذا كانت خالية [96]

وقد قضت محكمة النقض المصرية في أحد أحكامها على أن، القيود الواردة على التفتيش تنصرف إلى السيارة الخاصة بالطرق العامة فتحول دون تفتيشها إلا في الأحوال الاستثنائية التي رسمها القانون، طالما أنها في حيازة أصحابها فإذا كانت خالية وكان ظاهر الحال يشير إلى تخلى صاحبها عنها سقطت هذه الحماية وجاز تفتيشها وأن هذا لا يعد تفتيشاً بالمعنى الذي يبتغيه القانون وإنما ضرب من ضروب التحري عند مالك السيارة أو قائدها عله يهتدي إلى معرفة شيء من محتوياتها ولا جناح على الشرطة في ذلك .

---

[94] شرح قانون أصول المحاكمات الجزائية، ط1، مؤسسة نشر الثقافة القانونية، أربيل، 2003، ص 197

[95] أحمد المهدي، أشرف الشافعي، التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها ط1، القاهرة، 2007، ص 108

[96] التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2006، ص 589،

في تقديري ان التفتيش في الجرائم المعلوماتية يجب ان يتم بواسطة ذوي خبرة فنية لان اتلاف الادلة يمكن ان يتم دون قصد بواسطة الجهة التي تقوم باجراء التفتيش فمثلا فصل الجهاز عن التيار الكهربائي يمكن ان يقوم بفقدان بعض المعلومات هذا بجانب الاجراءات الاحترازية الفنية البحتة مثل نسخ معلومات الجهاز نسخة طبق الاصل والاحتفاظ بالاصل والعمل على النسخة.

ومن واقع تجربتي الشخصية في مجال الجرائم المعلوماتية ان التحري دائما ياتي بالمعلومات مطبوعة على اوراق اي يقوم التحري بطباعة الادلة وعرضها امام المحكمة والبينة الالكترونية يجب ان تقدم الكترونيا لان اي تلاعب بالبينة يمكن ان يتم اذا تمت طباعتها في الاوراق ويجب على المحاكم المختصة عدم قبول اي بينات الكترونية لا تقدم الكترونيا ابتداءاً.

المبحث الثالث : شروط الدليل الإلكتروني المستمد من التفتيش

كتب الدكتور على حسن الطوالبة أستاذ القانون الجنائي وعميد كلية الحقوق في البحرين إن الأدلة الإلكترونية ، إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات ، أو الراسم ، وإما أن تكون مخرجات غير ورقية أو أن تكون إلكترونية كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به ، أو الإنترنت بواسطة الشاشات أو وحدة العرض المرئي، ويكون الدليل باطلاً إذا حصل عليه عن طريق مخالفة القانون ، ولهذا الموضوع أهمية بالغة لما يترتب على بطلان الدليل من آثار، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم ، فإذ ما شاب التفتيش الواقع على نظم الحاسوب عيب فإنه يبطله ، والتفتيش الذي يقوم به المحقق بغير الشروط التي نص عليها القانون يعتبر باطلاً بطلانًا مطلقًا ولا يجوز التمسك بما ورد في محضر

التفتيش كما لا يجوز للمحكمة أن تعتمد عليه في حكمها ويقع عبء إثبات الجرائم المعلوماتية على عاتق النيابة العامة ، كما أن المدعي بالحق الشخصي يشارك النيابة العامة هذا العبء ، وفي أحيان أخرى ينقل القانون عبء الإثبات من النيابة العامة إلى عاتق المدعى عليه ، وأعطى المشرع الأردني النيابة العامة سلطة التحري وجمع الأدلة من خلال قانون أصول المحاكمات الجزائية ، وقد نصت المادة (17) منه على أنه: [97]

المدعي العام مكلف باستقصاء الجرائم وتعقب مرتكبيها.

ويقوم بذلك على السواء المدَّعون العامّون المختصون وفقًا لأحكام المادة (5) من هذا القانون) ، والدليل المتحصل من تفتيش نظم الحاسوب والإنترنت لا يكون مشروعًا ، ويعتبر باطلاً إذا تم الحصول عليه بغير الشروط التالية:

الشرط الأول:

يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات، إن أهم هدف للدستور هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير الحديثة نصوصًا تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها ، بحيث يتقيد المشرع بها عند وضع قانون أصول المحاكمات الجزائية ، فنص الدستور الأردني في المادة (10) منه على أن: (للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المُبيّنة في القانون ، وبالكيفية المنصوص عليها فيه ، ونص كذلك (تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية فلا تخضع للمراقبة أو التوقيف إلا في الأحوال المعينة في القانون) ، فهذه النصوص الواردة في الدستور تفرض على المشرع عند وضع قواعد

---

[97] علي حسن الطوالبة – التفتيش الجنائي على نظم الحاسوب والانترنت – عالم الكتب ط1، مرجع سابق ص 188.

الإجراءات الجنائية الالتزام بها وعدم الخروج عنها ، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام ، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها ، ونرى ضرورة أن يقوم المشرع السودانى بتشريع نصوص إجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب والإنترنت ، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانوني ، حماية للحقوق والحريات الفردية التي كفلها الدستور السودانى ، بالإضافة إلى المواثيق الدولية.

أما جزاء مخالفة القانون في الحصول على الأدلة فيترتب عليه جزاءات جنائية أو إدارية فضلاً عن الحكم بالتعويض ، فالموظف الذي يعهد إليه القانون بعمل فيتصرف على وجه مخالف يعد مقصرًا في عمله ومخالفًا في واجباته فيستحق المؤاخذة، والمهم هنا هو الجزاء الإجرائي إذ لا شك إن الدليل المستخلص عن طريق ارتكاب جريمة يكون باطلاً بطلانًا متعلقًا بالنظام العام ، ويجب على المشرع السوداني إعادة النظر في ما نص عليه قانون الإثبات لسنة 1994م فى المادة (10) ألفقره (1) البينة المتحصل عليها بإجراء غير صحيح حيث نصت على (مع مراعاة أحكام الإقرار والبينة المردودة لا ترد البينة لمجرد انه تم الحصول عليها بإجراء غير صحيح متى ما اطمأنت المحكمة إلى كونها مستقلة ومقبولة) فلابد من مراجعة هذه المادة اذا كانت ستطبق فى اثبات الجرائم المعلوماتية لان الاطمئنان ليس ليس حظ وافر امام الدليل القاطع الذى يجب ان يتوفر فى جرائم الحاسوب بما لا يدع مجال للشك . ففي فرنسا يرى جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفًا بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج، ما عدا حالات المحافظة على سر المهنة ، فإنه يكون في حل من الالتزام

بأداء الشهادة ، وفي هولندا يتيح قانون الحاسوب لسلطات التحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله كالإفصاح عن كلمات المرور السرية ، والشفرات الخاصة بتشغيل البرامج المختلفة ، أو حل رموز البيانات المشفرة وفي إطار مشروعية الأدلة الإلكترونية ، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة ، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية ، أم في مجال التنقيب في جرائم الحاسوب والإنترنت كأن يستخدم أعضاء التحقيق او كما هو مسمى لديهم **(الضابطة العدلية)** طرقًا معلوماتية في أعمال التنصت على المحادثات الهاتفية ، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ، ومن بينها الأدلة المتحصلة من الحاسوب والإنترنت ، بطريقة شرعية ونزيهة ، ونفس الشيء نجده في سويسرا وبلجيكا. وفي بريطانيا قامت الشرطة بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناءً على موافقتها ، وقد أجرت الشاكية عدة مكالمات هاتفية مع الشخص الذي كانت الشرطة تشك في ارتكابه الجريمة ، وقد تم تسجيل هذه المكالمات التي تضمنت موضوعات تدين المتهم ، لكن القاضي استبعد هذه التسجيلات على أساس أنها تمت من خلال شرك خداعي، أما في هولندا ، فإذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية ، فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات ، وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية، أما في اليابان فقد أصدرت محكمة حكماً أقرت فيه مشروعية التنصت للبحث عن الدليل ، حيث ضرورة التحريات ، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار،لكن الفقه الياباني ، يرى أن الأدلة الجنائية التي يتم الحصول عليها بطرق مشروعة يجب أن تكون

مستبعدة سواء كانت تقليدية أم أدلة حاسوب أم أدلة إنترنت .ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية ، الإكراه المادي والمعنوي في مواجهة المتهم ألمعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة ، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية ، كالتحريض على الغش أو التزوير ألمعلوماتي أو التجسس ألمعلوماتي ، والاستخدام غير المصرح به للحاسوب ، والتنصت ، والمراقبة الإلكترونية عن بُعد.

وتُعد من الطرق غير المشروعة أيضًا استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية ، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ، ومستمدة بطرق مشروعة ، ومدة حفظها محددة زمنيًا ، وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها ، وحق الشخص المعني في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة ، ولقد تضمن قانون الشرطة والإثبات الجنائي الإنجليزي لعام 1984م ، تحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تقبل أمام القضاء ، وتضمن كذلك توجيهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب ، فأوصت المادة (11) منه، بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسوب المقبولة في الإثبات طبقًا للقانون نفسه ، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في

وقت معاصر لهذا الأمر أم لا ، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيانات من الحاسوب لديه دافع لإخفاء الوقائع أو تشويهها .

الخطوات التفصيلية التي يجب على المحقق الجنائي الرقمي إتباعها في مسرح الجريمة الالكترونية مع توضيح الأساليب المستخدمة في جمع الأدلة الجنائية واستخراجها من أجهزة المتهمين وذكر لبعض لأدوات والمعدات لهذه المهمة.

لنفترض بأن جريمة وقعت في مكان ما، وقام أفراد الشرطة بإستدعاك بحكم وجود جهاز كمبيوتر في مسرح الجريمة، ومن المتوقع وجود إثباتات تدلنا على مرتكب الجريمة، ماهي الطريقة المثلى لفحص الجهاز بالتفصيل شارحاً الخطوات التي يجب تجنبها ولماذا دائماً نظن بأن عملية فحص الكمبيوتر للبحث عن الأدلة عبارة عن عملية سهلة ولكن في الحقيقة هي ليس كذلك وتحتاج لخطوات مطولة، إليكم تفاصيلها كالتالي بدايةً التحقيق الجنائي الرقمي أداة مهمة لاستخراج الأدلة في هذا الزمان، لأن المحقق الجنائي يكتشف ويستخرج ويسجل الدليل الحاسوبي. حيث يمكن استخدامه من قبل الحكومات، الجيوش، الشركات التقنية والبنوك... الخ. في هذه القضية لابد من فحص حاسوب الضحية لأنه قد يحتوي على بيانات مهمة قد تدلنا على المجرم مباشرةً، كالصور ،المحادثات المسجلة،البريد الالكتروني وخلافه ,التي قد تقدم في المحكمة كدليل ضد المذنب. فالإجراء المتخذ في مثل هذا النوع من القضايا يبدأ بالاستعداد بدراسة المعلومات المبدئية المقدمة عن القضية قبل التحقيق بعد ذلك يبدأ التحقيق وتحصيل الأدلة من مسرح الجريمة ,وأخيراً التحقيق بشكل مفصل واستخراج الأدلة الإلكترونية في المختبر الخاص بالتحقيق الجنائي الرقمي[98]...

نعرف المواقع التي زارها الشخص، أو أي سجلات محادثة متوفرة مثل: إم إس إن ياهو ،آي سي كيو، ... الخ التي قد تساعد في حل القضية. لا ننسى فحص أي

---

[98] علي حسن الطوالبة ، مرجع سبق ذكره ، ص 193.

مستندات أو أي قصاصات ورقية تحتوي على ملاحظات أو ربما أصابع الذاكرة USB أو أقراص خارجية الموجودة في مسرح الجريمة التي قد تساعد عملية التحقيق .والأهم من ذلك كله يجب على المحقق الجنائي كتابة كل شيء يحدث له سواء كان في مسرح الجريمة أو في المعمل، لأنه في بعض الأحيان وفي بعض القضايا تأخذ سنين لحلها وهذه المذكرات التي يسجلها المحقق قد تذكره لاحقاً اذا أمر بالتحدث للمحكمة أو خلافه.الآن وبعد الوصول لمسرح الجريمة، على المحقق حماية المنطقة التي يعمل عليها بأي حواجز تمنع دخول أي أحد لمنطقة عمله والعبث بالدليل، ويجب عليه عدم لمس أي شيء في مسرح الجريمة إلا المنطقة المكلف له بالتحقيق فيها، لأن لمس أي شيء أو ربما مجرد تحريك طاولة قد يعرقل عملية التحقيق على المحققين الآخرين في القضية. حسناً ، بعد ذلك يجب على المحقق أن يقوم بعملية لصق طوابع على جميع الأسلاك الموصولة بالحاسب أو اللابتوب وتسجيل ذلك على الطابعة، فعلى سبيل المثال يكتب على الطابع الملصق على سلك الفأرة " سلك الفأرة " . وبعد ذلك يجب عليه أن يصور الحاسب من كل جهة والمكان الموضوع فيه . لماذا؟ حتى في حال لو أردنا تشغيل الحاسب مره أخرى يجب أن يكون في نفس الوضعية التي كان بها وبنفس التوصيل .

بعد أن يتم ذلك يبدأ في البحث بجواره الحاسب عن أي ملاحظات على قصاصات ورقية التي قد تحتوي على بيانات مهمة مثل كلمة مرور أو أي شيء يفيدنا، لأن الحصول على مثل هذه المعلومات قد يساعد في تقصير مدة التحقيق على حساب عمليات كسر كلمة المرور وتخطيها في المختبر. الآن وبعد أن يتم جميع ما سبق يجب على المحقق فحص الحاسب، فإذا كان الحاسب مغلق لن يقوم بتشغيله ابداً ! لأن فعل ذلك سوف يحدث سجلات النظام بآخر موعد تشغيل وهذا سوف يفسد علينا القضية بأكملها ، ونفس الحال لو كان النظام يعمل فلن نقوم

بإغلاقه ، لان إغلاقه سوف يحدث سجلات النظام وننتهي في نفس المطاف! فيجب علينا التأكد من وضع الحاسب على سبيل المثال إذا كان محمول عن طريق الإشارات الضوئية للبطارية والهاردسك ووضع التشغيل، فلو كانت تومض وتدل على أن الحاسب يعمل وفي وضع الاستعداد على سبيل المثال فلن نتمكن من تشغيله ويجب على المحقق أن يقوم بنزع البطارية من الجهاز وبعد ذلك فصل سلك الشاحن من نفس الجهاز، لكن لو كان الجهاز يعمل والشاشة على سطح مكتب النظام فالوضع هنا مختلف، حينها يجب على المحقق أن يأخذ صورة للشاشة بإستخدام الكاميرا التي معه، ويدون جميع التطبيقات التي تعمل أمامه ، حتى إذا كانت شاشة توقف أو شاشة تطلب تسجيل كلمة المرور يجب عليه تدوين ذلك.

لنفترض بأن في الشاشة لدينا مطلوب أن ندخل كلمة مرور.. في هذه الحالة لا نقوم بأي عملية تخمين بل نقوم بسحب سلك الكهرباء الموصل إلى الحاسب وأخذه إلى المختبر، لكن في حال النظام كان يعمل بشكل طبيعي فهنا يجب أن نستمر , على المحقق أن يفعل شيئان فقط لا غير:

1. استخدام برنامج مثل , COFEE لاستخراج كافة السجلات الخاصة بالنظام عن طريق.USB
2. أخذ صورة للذاكرة المؤقتة عن طريق عملية crash dump على سبيل المثال أو باستخدام برنامج مثل LiveKd أو ربما ملفات عملية الإثبات.

على المحقق عدم العبث والدخول على أي ملف أو البحث في النظام بأي طريقة لأن فعل ذلك سوف يحدث السجلات الخاصة بالملفات والمجلدات وإضعاف الحاسب كدليل في المحكمة. بعد ذلك يجب على المحقق أن يفصل سلك الكهرباء عن الحاسب وتجهيزه للنقل إلى المختبر، مع التأكد بأن جميع الأسلاك الموصولة يوجد طابع عليها لتذكرينا بها وبمكانها بالتحديد .

جميع ماسوف يتم جمعه يجب أن يحفظ في أكياس خاصة ترجمتها الحرفية " أكياس الدليل – أو حافظة الدليل " حيث يوضع داخلها كل ما يمكن جمعه من أقراص ليزرية ، أصابع ذاكرة ... ,USB الخ. ويجب التعامل مع كل كيس كأنه " قابل للكسر " أي بحذر شديد لأن بدون الدليل لا يوجد لدينا أي قضية. أي جهاز إلكتروني يجب أن يحفظ في أكياس خاصة مضادة للشحنات الساكنة لتجنب إتلافها من قبل المصادر المغناطيسية .

حيث يجب أن يكون على الكيس مثل المسودة يتم تسجيل فيها مثلاً الشركة المصنعة والموديل و الرقم التسلسلي ويجب أن تكون هذه المسودة دوماً مع هذا الكيس. وايضاً مسودة أخرى تختص بمن أستلم الدليل " أي عملية الإستلام والتسليم والنقل " حيث يتم تسجيل فيها كل شخص أخذ الدليل إلى حين وصولها للمحكمة، يتم تسجيل في هذه المسودة من أخذ الدليل، متى ، وماهو الدليل , وأين ، وكيف ولماذا ! وهذه المسودة يجب ايضاً أن تكون دوماً برفقة الدليل داخل الكيس الآن وبعد أن تمت عملية جمع الأدلة من مسرح الجريمة وكل الأدلة المطلوبة موجودة لدينا في المختبر، يجب على المحقق إنشاء نسخة من الأدلة التي سوف يعمل عليها، لتجنب أي ضرر ممكن أن يحصل للدليل الأصلي من عملية التحقيق حيث الدليل الأصلي يجب أن يحفظ بعيداً لحين إستخدامه في المحكمة، وهذه الخطوة تعتبر خطوة مهمة حيث ليس من المعقول العمل على النسخة الأصلية من الدليل .ويجب على المحقق التأكد من النسخة المصنوعة من الدليل طبق الأصل تمام ولعمل ذلك يجب علينا إخراج الدليل من الحافظة في حالتنا هذه فان الدليل هو الحاسب ويجب علينا فك الحاسب مع تصويره وتدوين جميع ما يحدث قبل وبعد فكه لإستخراج القرص الصلب منه في سبيل عمل نسخة منه أو بالأصح نسختين، النسخة الأولى مكتبية حيث يتم العودة لها في حال حصول أي ضرر للنسخة

الأخرى ألا وهي نسخة العمل (هذا لايعني الإهمال لكن مجرد احتياط) مع التأكد بأن النسخة المأخوذة للقرص الصلب نظيفة جنائياً (بدون فيروسات – بدون ملفات تجسس ... – الخ) وفي خلال عملية النسخ يجب علينا إستخدام جهاز مانع الكتابة (Write Blocker –لتجنب كتابة أي بيانات على القرص الصلب الأصلي، حيث يفضل إستخدام نسخة عتادية منه وليس مجرد برنامج .

وللتأكد بأن النسخة المأخوذة مطابقة للنسخة الأصلية يجب على المحقق إستخدام طريقة أكواد التشفير (مثل (... – md5– sha :حيث تكون للصورة المأخوذة من النسخة كاملة ويتم مقارنتها بالقرص الصلب الأصلي. (يفضل عمل نسخ من نوع bit–stream حتى يمكننا إستعادة الملفات المحذوفة لو اضطررنا فعل ذلك ،بعد أن تتم عملية نسخ القرص الصلب والتأكد بأن النسخة مطابقة يستطيع المحقق البدء في استكشاف ملفات القرص الصلب براحة تامة ، دون القلق من إتلاف الدليل أو أي سبب آخر يمنعنا من إستخدام القرص الأصلي. في النهاية، أو أن أذكر الجميع بأن هذه الطريقة قد تختلف قليلاً لأنه في بعض الأحيان قد لا نحتاج لجلب جهاز الضحية إلى المختبر ويتم العمل عليه في مسرح الجريمة مباشرة على حسب أهمية القضية ، ومع التنبه بأن في بعض القضايا يتم مسح كافة محتويات القرص الصلب بكبسة زر واحدة إذا لم يكن المحقق متيقظ لذلك! التحقيق الأمن الجنائي الرقمي ليس فقط لاستخراج الأدلة من حواسيب المشتبه بهم أو الضحايا، بل هناك قضايا آخري مثل التهديدات الإلكترونية، النصب والاحتيال عن طريق الإنترنت، البرامج ,الفيروسات والباكدورات، قضايا الإختراق والتهكير ... الخ

المكونات القابلة للتفتيش

يعرف الحاسوب بأنه (مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلية طبقاً لبرامج تم وضعه مسبقاً

للحصول على نتائج معينة) وعرف أيضاً بأنه (جهاز إلكتروني يستطيع ترجمة عمليات إدخال البيانات وإخراج المعلومات وإجراء عمليات حسابية أو منطقية ويقوم بالكتابة على أجهزة الإخراج).

ويجب أن يتوفر في جهاز الحاسوب نوعين من القدرة ليسمى حاسوباً، إذ يجب أن يكون الحاسوب قادراً على القيام بالعمليات الحسابية والمنطقية طبقاً للتعليمات التي برمج عليها الحاسوب وتسمى هذه العملية بالمعالجة.

وقد تضمن بعض التشريعات تعاريف الحاسوب، فقد عرف قانون أدلة الحاسوب الجنوب أفريقي في مادته الأولى الحاسوب بأنه (أية أداة أو جهاز قادر على استلام البيانات بأي من الوسائل سواء كانت الميكانيكية أو الكهروميكانيكية أو الإلكترونية تدخل إليه وتتم معالجتها طبقاً للقواعد المنطقية أو الرياضية وخزنها ثم إخراج البيانات كنتائج لهذه المعالجة) وعرفته المادة الثانية من قانون إساءة استخدام الحاسوب السنغافوري بأنه (مجموعة من الأجهزة المترابطة مع بعضها البعض تدخل إليها البيانات بوسائل إلكترونية أو بصرية أو كهربائية وتقوم بتنفيذ مهام حسابية منطقية لهذه البيانات وخزنها ومن ثم إخراج النتائج).

ويتميز الحاسوب بخصائص عديدة منها السرعة إذ يستطيع الحاسوب أن يقوم بوظائفه بسرعة فائقة وهذه الخاصية توفر على الإنسان الكثير من الوقت والجهد ويعمل احتمالات الخطأ في أضق نطاق.

شروط قبول الدليل الالكتروني:-

أ- يجب ألا يوجد أساس معقول للاعتقاد أن البيان خاطئ أو غير دقيق ، بسبب الاستعمال الخاطئ وغير الملائم للظروف أو للغرض الذي يستخدم من أجله الحاسوب.

ب- يجب أن تكون جميع المكونات المادية للحاسوب عامله بدقة وعلى نحو متوافق كما ينبغي.

ت- إن أيًا من الشروط المحددة (التي تدخل في متطلبات القبول) المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة .

ولقد قضت محكمة الاستئناف الجنائي في إنكلترا بذلك ، حيث بينت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسوب ، ويتلخص الحكم بما يلي: (أنه يبدو لهذه المحكمة – أنه من الخاطئ رفض أو إنكار أية مزايا أو صلاحيات مقررة وفقًا لقانون الإثبات ، يمكن بمقتضاها التوصل عن طريق التقنيات الجديدة والوسائل الحديثة التأكد من صحة وصدق التسجيل ، حيث يمكن التثبت من ذلك ، وكذلك يمكن التعرف بوضوح على الأصوات المسجلة ، والمستخلص أيضًا هو أن الدليل وثيق الصلة بالموضوع ، من جهة أخرى ، يمكن قبوله ، ومن ثم تؤيد المحكمة قبول هذه الأشرطة ويجب أن ينظر دائمًا بعين الاعتبار إلى مثل هذا الدليل ، وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية.

يُشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة ، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين ، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية ، والمصغرات الفيلمية ، وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر ، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات ، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية ، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.

وجود إمكانية لمناقشة الأدلة الإلكترونية المستخرجة من الحاسوب والإنترنت

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لمناقشة أطراف الدعوى لها بحريه، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب ، أم كانت بيانات مدرجة في حاملات البيانات ، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية ، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة ، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات ، يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي ، لكن بصفة مباشرة أمام القاضي ، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الحواسيب، وأيضًا بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن تم سماع أقوالهم في التحقيق الابتدائي ، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم ، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم ، أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة وكشفًا للحق.

حجية الدليل الإلكتروني الناشئ عن التفتيش

إنَّ حجية المخرجات المتحصله من الحاسوب ، هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر، بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية، من قوة استدلالية في كشف الحقيقة.

لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي القوانين ذات الصياغة اللاتينية، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني، فإن حجية الأدلة الإلكترونية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات جرائم الحاسوب والإنترنت ، ولا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، وفي فرنسا مشكلة حجية المخرجات المتحصلة من الحاسوب على مستوى القانون الجنائي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة ويدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل أجهزة التصوير وأشرطة التسجيل وأجهزة التنصت، وقد قضت محكمة النقض الفرنسية: (إن أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي) ، وكذلك الحال بالنسبة لكل من ألمانيا وتركيا ولوكسمبورج واليونان والبرازيل وكل هذه الدول تخضع الأدلة الإلكترونية لحرية القاضي في الاقتناع الذاتي، بحيث تكون بمقدوره أن يطرح مثل هذه الأدلة رغم قطعيتها من الناحية العلمية ذلك عندما يجد أن الدليل الإلكتروني لا يتسق منطقيًا مع ظروف الواقعة وملابساتها.

أما في نظم دول الأنجلوسكسونية التي يحدد المشرع فيها أدلة الإثبات ويقدر قيمتها الإقناعية، فتأتى بريطانيا في طليعة هذه الدول التي تتبنى هذا النظام، بريطانيا، أصدرت قانون إساءة استخدام الحاسوب في عام 1990م، الذي لم يتناول الأدلة[99].

الناتجة عن الحاسوب، وربما كان السبب هو وجود قانون البوليس والإثبات الجنائي لسنة 1984م ، الذي حوى تنظيمًا محددًا لمسألة قبول مخرجات الحاسوب والإنترنت، كأدلة إثبات في المواد الجنائية ،وفي الولايات المتحدة الأمريكية تناولت

---

[99] الحجية القانونية للمستندات الالكترونية.

بعض القوانين حجية الأدلة الإلكترونية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسوب لسنة 1984م، الصادر في ولاية أيوا، من أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة 716/أ/16)، كما يتضح من قانون الإثبات الصادر في عام 1983م في ولاية كاليفورنيا، من أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات،وفي كندا، يمكن قبول السجلات الناجمة عن الحاسوب، إذا توافرت شروط معينة، وتنص المادة (29) من قانون الإثبات الكندي على عدد من الشروط التي يجب توافرها قبل عمل صورة من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان بإنه يشترط لكي تكون سجلات الحاسوب مقبولة بوصفها نسخًا حقيقية من السجلات الإلكترونية، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفًا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كافٍ. وتنص قواعد الإثبات الفيدرالية الأمريكية على أن النسخة المطابقة للأصل لها ذات حجية الأصل، أيًا كانت الطريقة أو الوسيلة المستخدمة في النسخ، كالطباعة والتصوير والتسجيل الميكانيكي والتسجيل الإلكتروني، بما يسمح بقبول مخرجات الحاسوب في الإثبات، والغالب الأعم في القضاء الأمريكي أنه يُعول على قبول دليل السجلات المحتفظ بها على الحاسوب أما في القوانين ذات الاتجاه المختلط ، وهي التي تجمع ما بين النظامين اللاتيني والانجلوسكسوني، فيعتمد النظام المختلط على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر أو يشترط في الدليل شروطًا في بعض الأحوال أو

يعطي القاضي الحرية في تقدير الأدلة القانونية، مثل القانون الإجرائي الياباني وقد حصر المشرع الياباني طرق الإثبات المقبولة بما يأتي: [100]

(أقوال المتهم، وأقوال الشهود، والقرائن، والخبرة)، أما بالنسبة لأدلة الحاسوب والإنترنت، فيقرر الفقه الياباني، أن السجلات الإلكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب والإنترنت، سواء كانت هي الأصل أم كانت نسخة من هذا الأصل وتنص المادة (113) من قانون الإجراءات الجنائية الشيلي، على إمكانية استخدام الأفلام السينمائية، والحاكي، (الفونوغراف)، والنظم الأخرى الخاصة بإنتاج الصورة والصوت والاختزال وبصفة عامة أية وسائل أخرى، قد تكون ملائمة، ووثيقة الصلة، وتفضي إلى استخلاص المصداقية، يمكن أن تكون مقبولة كدليل إثبات ويرى الفقه الشيلي، أن الدليل الناتج عن الحاسوب والإنترنت، يمكن أن يكون مقبولاً في المحكمة، كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، وحجة الفقه الشيلي تستهدف توسيع مظلة الوسائل العلمية الحديثة في الإثبات، لتغطي العناصر الإثباتية الناتجة عن جرائم المعلوماتية تعد مراقبة المكالمات السلكية واللاسلكية – تحت رقابة القضاء- من الوسائل الملائمة لضبط ما يفيد في كشف الحقيقة أحيانًا، وقد أحاط المشرع إجراء المراقبة الهاتفية واللاسلكية بضمانات معينة فلا يجوز إجراؤها إلا بأمر مسبب من القضاء وبصورة مشروعة لكن ما القوة الإثباتية للتسجيلات الصوتية المُسجلة إلكترونيًا .إن الصوت عند تسجيله إلكترونيًا ، لا يحتمل الخطأ، ويصعب التلاعب به، ويمكن للخبراء أن يكتشفوا أي تلاعب أو خداع بوسائل تقنية عالية الكفاءة، ومن

---

[100] خالد المهيري-التحقيق الجنائي العلمي في الجريمة التقليدية والمعلوماتية –الطبعة الثانية – دار الكتب المصري الحديث القاهرة سنة 1992م ص 29 ومابعدها

ثم يمكن القول بأن التسجيل الصوتي الممغنط يمكن أن تكون له حجة دامغة في الإثبات ويمكن باستخدام تكنولوجيا للحواسيب الحديثة والإنترنت وطرق الاتصال المعلوماتي السريع، أن يستخدم تسجيل الفيديو لإثبات تُهم استعمال القسوة أو إساءة استعمال السلطة من قبلِ أعضاء الضابطة العدلية ضد المواطنين، كما يمكن استخدامها لتسجيل عمليات القبض والتفتيش وضبط الأدلة والآثار الأخرى الناجمة عن الجريمة تسجيلاً دقيقًا، كما يمكن استخدامها كتقنية عالية الكفاءة لعمل المعاينات اللازمة لمسرح الجريمة ويشترط الفقه لمشروعية الدليل المستمد من المراقبة والتسجيل عدة شروط.

الدليل المستمد من التسجيل او المراقبه

أ- إذا لم يكن التسجيل منطويًا على اعتداء على حق يحميه القانون، فيكون الدليل في هذه الحالة مشروعًا، ويمكن للمحكمة أن تستند إليه في قضائها بالإدانة أو بالبراءة تحديد دقيق للشخص أو لهوية الشخص المراد تسجيل أحاديثه أو بريده الإلكتروني كل ما كان ذلك ممكنًا في حالة الإنابة للتفتيش.

ب- تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرح لها بذلك، والمدة الجائز خلالها التقاط الحديث خلاله.

ت- ويمكن استخدام "حاسوب الجيب" على أنه " أداة تبرئة" إذ يمكن أن تكون التوقيعات المشفرة من خلاله دليل براءة غير قابل للدحض في مواجهة أية اتهامات باطلة، فلو أن شخصًا ما أتُهم بأمر معين أو جريمة معينة فبإمكانه أن يُدافع عن نفسه من خلال ما هو مُسجل من أقوال وأفعال في أي وقت.أما البريد الإلكتروني، فعند إرسال رسالة من خلاله فإنه يكون لدى الشخص المستقبل توقيعًا رقميًا (إلكترونيًا)، ويكون المستقبل وحده القادر على استعماله، وسيتم تشفير الرسالة، بحيث لن يتمكن من حل شفرتها إلا الشخص المقصود إرسالها

إليه، ويمكن لهذه الرسالة أن تكون معلومات من أي نوع، مشتملة على الصوت والفيديو، أو تحويلات بنكية، وسيكون بإمكان متلقي الرسالة أن يتأكد من أن الرسالة مرسلة بالفعل من الشخص الذي أرسلها، وتحديد وقت إرسالها بالضبط، وأنها لم تتعرض لأي تلاعب، وأن الآخرين لا يستطيعون فك شفرتها، وبالتالي يمكن استخدام هذه المعلومات كحجة في الإثبات الجنائي ويستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما، أن يلفق أو يزور المفترض كتابة أو إرسال الوثيقة فيه فسيكون هذا التلفيق أو التزوير قابلاً للكشف، وسوف يرد ذلك الاعتبار للقيمة الإثباتية للصور الفوتوغرافية والفيديوية، ولقد أضاف علم التصوير للإثبات الجنائي قيمة علمية بما له من أثر في نقل صورة صادقة للأماكن والأدلة إلى كل من يعنيه الأمر، اعتمادًا على آلة التصوير والأفلام التي لا تعرف الكذب، بيد أنه لا يمكن إنكار الآثار السلبية والخطيرة التي تنشأ عن استخدام هذه الوسائل، لما قد يحدثه في الحياة الخاصة إذا لم توضع له الضوابط الكافية،وتختلف حجية التوقيع الإلكتروني في الإثبات المدني عنه في الإثبات الجنائي، حيث يخضع في الإثبات المدني لقواعد شكلية، أما في الإثبات الجنائي فيخضع تقديره لمطلق سلطة قاضي الموضوع، واقتناعه بصحته وقوته الإثباتية، كما أن وجود نظام تسجيل الدخول في شبكة الإنترنت يسمح بتحديد الأشخاص الذين دخلوا أو حاولوا الدخول بعد ارتكاب الفعل الجرمي، وتعد حالات ضبط مرتكب الفعل متلبسًا نادرة أو أنها وليدة الصدفة، وحتى لو تم ضبطه متلبسًا، فقد يرجع ذلك إلى خطأ في نظام الحاسوب أو الشبكة أو الأجهزة الأخرى، أو عن طريق مراقبة الشرطة بعد ملاحظة وجود بعض الاعتداءات، والفقه الفرنسي يعتبر انتهاك نظام الأمن لبعض المواقع المحمية، دليل حتمياً وقرينة قاطعة على وجود القصد الجرمي وسوء نية مرتكب الفعل، ويمكن للماسحات الضوئية،

وطابعات الليزر أن تكون أداة ارتكاب الجريمة، ففي عام 1994، قام أحد الأشخاص في مدينة دلاس الأمريكية بتزوير أجازات قيادة سيارات التاكسي باستخدام الماسحات الضوئية، وطابعات الليزر، كما جرت محاولات لإصدار بطاقات التأمين، وأوامر صرف مالية، وبعض أنواع الصكوك من خلال استخدام برمجيات الرسوم المتطورة، وأنظمة الطباعة المتخصصة.

إن المحاكم الجنائية قد لا تواجه مشاكل في تعاملها مع الأدلة الجنائية الإلكترونية الرقمية، وذلك للأسباب التالية:-

أ- الثقة التي اكتسبها الحاسوب والإنترنت والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات-ارتباط الأدلة الجنائية الإلكترونية وآثارها بالجريمة موضوع المحاكمة.

ب- وضوح الأدلة الإلكترونية، ودقتها في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والسلوك الإجرامي.

ت- إمكانية تعقب آثار الأدلة الإلكترونية والوصول إلى مصادرها بدقة.

ث- قيام الأدلة الإلكترونية على نظريات حسابية مؤكدة لا يتطرق إليها الشك مما يقوي من تقنية الأدلة الإلكترونية.

ج-الأدلة الجنائية الإلكترونية يدعمها- عادة- رأي خبير- وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرهاالقضاء.

عليه لابد من وجود توصيات أهمها كما نرى يتضمن الأتي:- [101]

لكي يُعد الدليل المستخلص من تفتيش وضبط نظم الحاسوب والإنترنت مشروعًا لا بد من توافر ثلاثة شروط في الدليل الإلكتروني المستمد من التفتيش وهي:

[101] هلالي عبدالله –التزام الشاهد بالعلام في الجرائم المعلوماتية دراسة مقارنة –دار النهضة العربية –القاهرة سنة 2000م ص 23

أ- يجب الحصول على الدليل المستمد من التفتيش بصورة مشروعة غير مخالفة لأحكام الدستور ولا القانون يجب أن تكون الأدلة الإلكترونية غير قابلة للشك أي يقينية.

ب- إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسوب والإنترنت.

ت- لقد أكدت التوصية التي أصدرها المجلس الأوروبي لعام 1995م، والخاصة بمشاكل الإجراءات الجنائية الوطنية على ضرورة الأخذ بالتوصيات التالية لكي تلائم النصوص القانونية التطور الحاصل في هذا المجال:

1- أن توضح القوانين إجراءات تفتيش أجهزة الحاسوب وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

2- أن تسمح الإجراءات الجنائية للجهات القائمة على التفتيش بضبط برامج الحاسوب والمعلومات الموجودة في الأجهزة وفقًا لذات الشروط الخاصة بإجراءات التفتيش العادية.

ومن أجل ضمان حفظ أسرار المدعى عليه غير المتعلقة بالجريمة من الاطلاع عليها يجب إتباع القائم بالتفتيش التعليمات التالية : [102]

أ- على القائم بالتفتيش أن يلتزم واجب الحيطة والحذر أثناء التفتيش فلا يطلع إلا على الأشياء أو الأماكن التي يحتمل أن يجد فيها بيانات أو برامج أو أشياء أو أدلة أو براهين لها علاقة بالجريمة.

ب- على المحقق أن لا يسترسل في الإطلاع عما ظهر أمامه صدفة.

ت- أن يحاول المحقق -ما وسعه الجهد-عدم اطلاع غيره على محتويات الحاسوب محل التفتيش.

[102] عبدالله حسين على محمود تجراءات جمع الادلة في محال جريمة سرقة المعلومات –بحث مقدم للمؤتمر العلمي الاول حول الجوانب القانونية والامنية للعماليات الالكترونية –محور القانون الجنائي –دبي –خلال الفترة 28/26 ابريل 2003م ص 616

ث- ضرورة إصدار دليل إرشادي تقني وقانوني حول صور جرائم الحاسوب والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية ومواصلة تحديث هذا الدليل بشكل دوري وكلما دعت الحاجة لذلك وتعميمه على العاملين في مجال التحقيق في الميدان وعلى أجهزة القضاء، والاستفادة من الدليل الصادر عن المنظمة العالمية للشرطة الجنائية الإنتربول.

حالات تفتيش مسرح الجريمة الالكتروني:

أن تفتيش مسرح الجريمة وما يتصل به من أماكن وضبط المحرزات ذات العلاقة بالجرم أمور تنظمها القوانين، ويثور التساؤل حول مدى انطباق القواعد القائمة على حالة تفتيش نظم الكمبيوتر وقواعد البيانات، ليس ذلك فحسب ، بل تثير أهمية الخبرة في هذا الحقل إذ كما يرى احد أشهر محققي التحقيقات الفدرالية الأمريكية أن الخطأ في تفتيش وضبط الدليل قد يؤدي إلى فوات فرصة كشف الجريمة أو فوات فرصة الإدانة حتى مع معرفة الجاني.

أن تفتيش نظم الحواسيب تفتيش للفضاء الافتراضي وأوعية التخزين، تفتيش للإجراءات التي يحفظها الجهاز أن كان مزودا بحافظات الكترونية للعمليات المنجزة عبره، وهو أمر يتعلق بالقدرة على تحديد المطلوب مسبقا، لان التعامل وفق المسلك الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات لأنها خارج نطاق أمر التفتيش والضبط أو قد تنطوي الإجراءات على كشف خصوصية البيانات المخزنة في النظام.

البيانات المخزنة داخل النظم ليس جميعا تتصل بجريمة الاعتداء على النظام، منها بيانات خاصة وأخرى ذات قيمة إستراتيجية، لهذا اهتم الخبراء القانونيون

بمخاطر الاعتداء على الخصوصية أو الحياة الخاصة في معرض الكشف عن الدليل أو في معرض الإقرار باستخدام دليل ذي طبيعة الكترونية وفي دولة ليس ثمة بعد قواعد لحماية الخصوصية سواء من حيث تنظيم أعمال جمع وتخزين ومعالجة ونقل البيانات، أو من حيث حقوق الدخول إليها وحق أصحابها بسلامتها وصحتها وتعديلها، أو من حيث إقرار الحمايات الإدارية التنظيمية والمدنية والجزائية لهذه البيانات، يكون ثمة صعوبة في حماية الخصوصية ويكون ثمة احتمالات اكبر لإهدار الأدلة غير القانونية ونشوء نزاعات في هذا.

ج- الشهـادة :

الشهادة في مجال الجريمة المعلوماتية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية وامر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق ، والاصل ان يطلب الخصوم سماع من يرون من الشهود وللمحقق ان يدعو للشهادة من يقدر ان لشهادته أهمية ، وله أن يسمع أي شاهد يتقدم من تلقاء نفسه.

والشاهد في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الالي والذي تكون لديه معلومات جوهرية أو هامة لازمة للدخول – الولوج- في نظام المعالجة الالية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخلة ويطلق على هذا الشاهد أسم "الشاهد المعلوماتي" وذلك تمييزاً له عن الشاهد التقليدي .

والشاهد المعلوماتي بهذا المفهوم قد يكون واحدا من عدة طوائف أهمها :- [103]

أ- مشغلو الحاسب الالي :

---

[103] عبدالله حسين على محمود ،مرجع سابق ، ص 619

وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الالي والمعدات المتصلة به واستخدام لوحة المافتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج .

ب- المحللون :

والمحلل هو الشخص الذي يحلل الخطوات ويقوم يتجميع بيانات نظام معين وتحليلها الي وحدات منفصلة واستنتاج العلاقات الوظيفية منها ، كما يقوم كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الاماكن التي يمكن ميكنتها بواسطة الحاسب.

ت- المبرمجون :

وهم الاشخاص المتخصصون في كتابة أوامر البرنامج ويمكن تقسيمهم الى فئتين :-[104]

الفئة الأولى :-

هم مخططو برامج التطبيقات ويقومون بتحويلها الي برامج دقيقة وموثوقة لتحقيق هذه المواصفات .

الفئة الثانية :-

هم مخططو برامج وادخال أي تعديلات أو إضافات لها .

ث- مهندسو الصيانة والاتصالات :

وهم المسئولون عن أعمال الصيلنة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به

[104] محمد فهمي –الموسوعة الشاملة لمصطلحات الحاسب الالكتروني –مطابع المكتب المصري الحديث-سنة 1991م ص

ج- مديرو النظم :

وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

الإقرار بحجية الوسائل الالكترونية في الاثبات [105]

تكاد تجمع كافة النظم القانونية في الوقت الراهن على حجية الملفات المخزنة في النظم ومستخرجات الحاسوب والبيانات المسترجعة من نظم الميكروفليم والميكرفيش وحجية الملفات ذات المدلول التقني البحت ، والاقرار بصحة التوقيع الالكتروني وتساوية في الحجة من التوقيع الفيزيائي والتخلي شيئاً فشيئاً على اي قيود تحد من اثبات في البينة التقنية والسنوات القليلة القادمة ستشهد تطوراً ايضاًفي الاتجاه نحو قبول الملفات الصوتية والتناظرية والملفات ذات المحتوي المرئي وغيرها .

لذا اتجهت معظم التشريعات الي قبول الوسائل الالكترونية كبينه في الدعاوى المصرفية ،وتجدر الإشارة الي ان المشكلة لاتزال تكمن في التعاطي الجزئي مع تدابير عصر المعلومات التشريعية .

سلطة القاضي الجنائي في قبول الدليل الالكتروني

تختلف سلطة القاضي الجنائي في تقرير أدلة الاثبات من دولة الي أخرى حسب ما كل من دولة من الاثبات وهناك نظامان للادلة المقبولة للاثبات :-

1- نظام الاثبات المقيد او المحدد : فيه تكون الادلة محصورة ومحددة سلفاً من قبل المشرع .

2- نظام الادلة الاقتناعية : يعرف بالمرحلة الوجدانية او مرحلة حرية الاقتناع في هذا النظلم يترك للقاضي الحرية في ان يؤسس حكمه على اي دليل وفقاً لقناعته الشخصية .

[105] يونس عرب –حجية الاثبات بامستخرجات الالكترونية في القضايا المصرفية ص 307 ومابعدها

3-نظام الاثبات المختلط : عبارة عن مزج بين الحرية في استخلاص الدليل وبين التقييد وينتمى القانون السوداني لهذه المدرسة الاخيرة .

الادلة المعلوماتية في المواد الجنائية .

مع ازدياد الاعتماد على نظم الكمبيوتر والشبكات في الاعمال اثيرت ولا تزال تثار مشكلة امن المعلومات ، أي حماية محتواها من انشطة الاعتداء عليها ، سواء من داخل المنشاة او من خارجها ، وانماط الاعتداء عديدة تبدأ من الدخول غير المصرح به لملفات البيانات الى احداث تغيير فيها وتحوير بمحتواها او اصناع بيانات وملفات وهمية ، او اعتراضها اثناء نقلها ، او تعطيل عمل النظام ، او الاستيلاء على البيانات لاغراض مختلفة او احداث تدمير او احتيال للحصول على منافع ومكاسب مادية او لمجرد الاضرار بالاخرين وحتى لاثبات القدرة واحيانا مجرد انشطة تستهدف المزاح الذي سرعان ما يكون عملا مؤذيا يتجاوز المزاح.

والحماية من هذه الاعتداءات واثبات قدرة النظام على التعامل الآمن مع البيانات يثير مشكلات اجرائية عديدة في معرض تفتيش نظم الحاسوب او تقديم الدليل في الدعوى الجزائية ، طبعا في النظم القانونية التي تنص على تجريم افعال الاعتداء على المعلومات انظر دراستنا جرائم الكمبيوتر المنشورة في مجلة البنوك في الاردن خلال عام 1999 - ، وحيث ان هذه الدراسة تتناول الاثبات ، فان من مقتضى وموجبات الموضوع التعرض للاثبات في الدعاوى الجزائية باستخدام الادلة ذات الطبيعة التقنية طبعا في حدود المساحة المتاحة مع الاشارة الى حاجة الموضوع لدراسة شاملة اكثر تخصصا .[106]

---

[106] دكتور يونس عرب-دراسة فى مسائل وتحديات الاثبات-الاردن مجلة البنوك الاردنية

الفصل الرابع

الخبرة في الجرائم الالكترونية

المبحث الاول:الخبرة في الجرائم الالكترونية

لقد تعاظم الاثبات العلمي للدليل مع ظهور الجرائم المعلوماتية وضرورة اشتقاق الادلة الرقمية المطلوبة للاثبات في هذه الجرائم وكشف أنماط الجرائم المرتكبه باستخدام الحاسب الالي ، وهو الدور الذي يطلع به الخبراء القانونيون والمختصين ، فأصبح انشاء " المعامل الجنائية الرقمية " مطلباً ملحاً لفحص الادلة الرقمية ولتقييم عملية الاثبات الرقمي وتحليل الجرائم في نطاق ما يعرف باسم نظرة

الخبرة الامنية، وعلى الرغم من أهمية الدليل إلا إن الجرائم المعلوماتية نظراً لحداثتها النسبية لم تأخذ القدر الكافي من الشرح وتقنين اجراءات اثباتها سواء من الناحية القانونية او الفنيةوهو ما القي علي عاتق المعنيين بكشف وتحقيق هذه الجرائم عبئا ثقيلاً [107]

تقوم الخبرة في العصر الراهن بدور بارز في عملية الاثبات نظراً لما شهده هذا العصر من تطور علمي وتكنولوجي لحد وصفه بعصر المعلومات لذا سنتناول في هذه الدراسة موضوع الخبرة في فرعين كل فرع مستقل وذلك على النحو التالي : **[108]**

أولاً : ماهية الخبرة

الخبرة هي اجراء يتعلق بموضوع يتطلب الالمام بمعلومات فنية لاستخلاص الدليل منه

او هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الاثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها الي مساعدة فنية أو ادارية التي قد لا تتوافر عند المحقق والقاضي المختص بأنها "الاستشارة الفنية التي يستعين بها القاضي او المحقق كما عرفها البعض بحكم علمة وثقافته لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها الي معرفة أو دراية علمية خاصة لا تتوافر لديه والخبرة الفنية تعتبر إجراء من إجراءات التحقيق بحسب الأصل ".[109]

وبما ان تقرير الخبير يعتبر والخبرة كدليل في الاثبات تتصرف الي راي الخبيرالذي يثبته في تقريره فاللمحقق الاستعانة بالخبراء من الادلة الفنية فان اجراء ندب الخبير

---

[107] ممدوح عبدالحميد عبدالمطلب –البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الالي والانترنت –دار الكتب القانونية –مرجع سابق ص 9

[108] مامون سلامة-الاجراءات الجنائية في التشريع المصري –الجزء الاول دار النهضة العربية القاهرة سنة 2001م ص 645

[109] امال عثمان –الخبرة في المسألة الجنائية رسالة دكتوراة كلية الحقوق جامعة القاهرة 1964م ص 28 ومابعدها

هو من اجراءات جمع الادلة ليستطلع رأيهم في بعض الامور التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهى بإصدار قرار بأن لا وجه لأقامة الدعوى أو بإحالتها الي محكمة الموضوع ،واما الخبرة في مرحلة المحاكمة فإنها تساعد القاضي في تكوين عقيدته للفصل في القضية .[110]

والخبير هو كل شخص له دراية خاصة بمسألة من المسائل وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية او علمية لايشعر المحقق بتوافرها في نفسة فيمكنه ان يستشير فيها خبيراً كما هو الحال في تقرير الصفحة التشريحية في جرائم القتل او تحليل المادة المطعومة في جريمة تسمم او فحص لخطوط الكتابة المدعى بتزويرها[111]

أهمية الإستعانة بالخبراء :

تكمن أهمية الخبرة في انها تنير الطريق للقاضي الذي يهتدى به لتحقيق العدالة خاصة في المجال الجنائي ،لذا فقد تم الاهتمام بالموضوع في كل من مصر والسودان بتنظيم اعمال الخبرة فقد أجاز قانون الاجراءات الجنائية المصري في المادة 29 منه وكذلك قانون الاجراءات الجنائية السوداني لسنة 1991م الاستعانة بالخبراءاثناء التحرى والتحقيق ، ولم يحظر كل من القانونين على المحاكم ان تستعين بالخبراء وبالتالي فإنه يجوز دائماً للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم ،ولكن إذا كان الطلب مقدماً من احد الخصوم لايجوز رفضه الا اذا كان عديم الفائدة ، وذلك لتعليق الامر بحق المتهم في الدفاع

[110]مامون سلامة- الاجراءات الجنائية في التشريع المصري –الجزء الاول دار النهضة العربية القاهرة سنة 2001م ص 645
[111]فتحي عبدالستار –شرح قانون الاجراءات الجنائية –دار النهضة العربية القاهرة سنة 1986 ص 332

وكون تعيين الخبير هو طريق من طرق الاثبات المتاحة للخصوم لا يجوز حرمانهم من الانتفاع به لتأييد طلباتهم .[112]

واذا كان للخبرة تلك الاهمية في الجرائم التقليدية فإن اهميتها تزداد وتصبح ضرورية بل وحتميه في اثبات الجرائم الالكترونية فالخبرة وسيلة من وسائل الاثبات التي تهدف الي كشف بعض الدلائل او الادلة (3) او تحديد مدلوها بالاستعانة بالمعلومات العلمية.

وهي بحث لمسائل مادية او فنية يصعب على المحقق ان يشق طريقة فيها ويعجز عن جمع الادلة (4) بالنسبة لها بالوسائل الاخري للإثبات

ومنذ ظهور جرائم الحاسب الالي تستعين الشرطة وسلطات التحقيق او المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الالي وذلك بغرض كشف غموض الجريمة او تجميع أدلتها والتحفظ عليها ، او مساعدة المحقق في إجلاء جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ويلاحظ ان نجاح الاستدلالات واعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هولاء الخبراء .

ويجب الاشارة الى ان الاجراءات الاولية التي يقوم بها أهل الخبرة في مرحلة جمع الاستدلالات لاتعد من قبل الخبرة إذ تودي دون اتباع الاجراءات الشكلية التي اوجبها القانون وهي الندب من سلطة التحقيق و أداء اليمين الا انه يجوز للمتحريين والمحققين الاستعانة بالخبراءوتحليفهم اليمين اذاخيف الا يستطاع فيما بعد سماع شهادتهم بيمين وذلك يتم بواسطة النيابة[113] .

---

[112]نبيل عبدالمنعم جاد –اسس التحقيق والبحث العلمي مرجع سابق ص 191

[113])المادة 29\2 من قانون الاجراءات الجنائية المصري والمادة 40 من قانون الاجراءات الجزائية الاتحادي الاماراتي

واهمية الاستعانة بالخبير في مجال الجرائم الاكترونية تظهر عند غيابه فقد تعجز الشرطة عن كشف غموض الجريمة وقد تعجز هي او جهة التحقيق على جمع الادلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل او الاهمال عند التعامل معه .

مجالات الخبرة بالنسبة للجرائم الالكترونية

افرز التطور الهائل في مجال تكنولوجيا المعلومات والاتصالات في عصر المعلومات العصر الرقمي او الالكتروني العديد من الانشطة المستحدثة التي تتم باستخدام الوسائل الالكترونية والتي قوامها نظم وبرمجيات الحاسب الالي والشبكات الحاسوبية وشبكات الاتصالات العالمية الانترنت كاعمال التجارة الالكترونية والمصارف والاعمال المصرفية الالكترونية والادارة الالكترونية والمحكومة الالكترونية مما ترتب علية ان تتنوع الجرائم التي تقع علي هذة العمليات وفقا لنوع الوسائل الالكترونية المستخدمة في ارتكابها .

ومن امثلة هذه الجرائم

أ– تزوير المستندات المدخلة في انظمة الحاسبات الالية او الناتجة بعد المعالجة .

ب– التلاعب في البيانات .

ت– التلاعب في البرامج الاساسية او برامج التطبيقات .

ث– الغش اثناء نقل وبث البيانات .

شروط صحة اعمال الخبرة الفنية ومدى حجيتها

نظراً لاهمية البالغة للخبرة والدور الذي يلعبه الخبير في عملية الاثبات في المجال الجنائي فقد حرصت معظم التشريعات على تنظيم الخبرة ووضع شروط

وضوابط لها بعضها يتعلق بالخبير وبعضها يتعلق بمدى حجية تقريره وهو ما سنعالجة علي النحو التالي :

شروط خاصة بتعيين الخبير : (السودان نموذج)

أ- ان يكون سودانيا متمتعا بالاهليه المدنيه الكاملة .

ب- ان يكون حائزا لدرجة بكالوريوس من احدى الجامعات المعترف بيها في مادة القسم الذي يطلب التعيين فيه او شهادة تعتبر معادلة لهذة الدرجة من الجامعة او معهد علمي معترف به .

ت- أن يكون مرخصاً له بمزوالة المهنة في النوع الذي يرشح للتعين فيه .

ث- ان لا يكون قد ادين في أمر مخل بالشرف والأمانه.

ج-ان يكون محمود السيرة ،وحسن السمعة (حسن السير والسلوك).

وهذا ويعتبر خبراء الادلة الجنائية والطب الشرعي فيما يختص بالجرائم المتعلقة بالأعمال التي يباشرونها وفي أثناء قيامهم بها خبراء بحكم التخصص .

لايجوز لهولاء الخبراء الجمع بين وظيفتهم اخري لا تتفق وكرامتهم واستقلالهم في عملهم .

والجدير بالذكر ان المشروع السوداني لم يعط شروطاً خاصة لتعيين الخبراء ، ويتضح في شان تنظيم الخبرة أمام المحاكم حيث "يجوز ان يتولى اعمال الخبرة امام المحاكم موظفون فنيون يعينون في الداخلية من بين المتخصصين في اعمال الخبرة ،ويتفرغ هولاء الموظفين للأعمال المذكورة ويخضعون في أداء مهمتهم للأحكام المنصوص عليها في أداء واجبهم العلمي الرسمي .

كما ان الخبير لايشترط فيه فقط كفاءة علمية عالية في مجال التخصص بل يجب ان يضاف الي سنوات من اعمال الخبرة في المجال الذي تميز فيه وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الالي.

فقد يتعلق الامر بتزوير المستندات او بالتلاعب في البيانات او جريمة من جرائم الاموال او الغش اثناء نقل او بث البيانات او الاعتداء على حرمة الحياة الخاصة او عرض صور او أفلام مخلة بالاداب العامة.[114]

أداء اليمين :

يجب لصحة تقرير الخبير أداء اليمين لحمله على الصدق والامانه في عمله ، وبث الطمأنينةفي أرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية الاطراف في الدعوى ولذلك لا يغنى عن هذا الإجراء أي ضمانه أخرى من الضمانات. [115]

فلقد أوجب القانون أن يحلف الخبير اليمين قبل أداء مهمته امام المحكمة وإلا كان العمل لاغيا ولقد استقر الفقه والقضاء على ان أداء الخبير لليمين يوم تسلمه العمل يغنى عن أدائه اليمين عند مباشرة كل مهمة وان كان لا تثريب على المحكمة ان استحلفته اليمين قبل أداء مهمته بعينها [116]

بمعنى انه عند حضور الخبير امام المحكمة لا يلزم ان يحلف يمين الشاهد إذ تكفى اليمين التي حلفها كخبير.[117]

---

[114]محمد ابو العلا عقيدة –التحقق وجمع الادلة في مجال الجرائم الالكترونية –مرجع سابق- ص 28
[115].احمد ابو القاسم –الدليل الجنائي المادي ودورة في اثبات جرائم الحدود والقصاص-مرجع سابق –ص 377
[116]نصت المادة 97 من قانون الاجراءات الجزائية الاماراتي والمادة 76 من قانون الاجراءات المصري علي "يجب على الخبراء ان يحافو امام قاضي التحقيق يمينا علي ان يبدوا رايهم بالذمة وعليهم ام يقدموا تقريرهم كتابه"
[117]محمد محمود مصطفي شرح قانون الاجراءات الجنايئة دار مطابع الشعب القاهرة سنة 1963م ص 348

فان كان الخبير من غير الخبراء المعينين بالقانون او كان اسمه غير مقيد في الجدول يجب في هذه الحالة استحلافه اليمين بأن يؤدى عملة بالصدق والامانه. [118]

وقد قضت محكمة النقض المصرية بأنه "... لما كانت المادة 86 من قانون الاجراءات الجنائية قد اوجبت ان يحلف الخبير يميناً امام قاضي التحقيق على ان يبدى رأيه بالذمة الا انه متي كان الخبير قد مثل امام المحكمة وحلف يميناً قبل سماع شهادته وكانت شهادة الخبير في حد ذاتها حقيقتها تقرير فني يتناول كل من قام به من اعمال تحضيرية والنتيجة التي انتهى اليها في تقريره فانه لايعيب الحكم ان عول على تقريراللجنة مادام اعضاؤها قد مثلوا امام المحكمة وحلف كل منها يميناً قبل سؤاله بشأن ما أجراه من أعمال الخبرة في الدعوى ...." [119].

المبحث الثانى : شروط صحة اعمال الخبرة الفنية ومدى حجيتها

تقرير الخبير:

وبعد إنتهاء الخبير من ابحاثه وفحوصاته يعد تقريراً يضمنه خلاصة ماتوصل اليه من نتائج بعد تطبيق الاسس و القواعد العلمية الفنية على المسائل محل البحث ، ونظراً لما تتسم به الاجراءات الجنائية من طابع السرعة وجب على الخبير ان يقدم تقريره في أقرب وقت ، ولذا على المحقق ان يحدد ميعاداً للخبير ليتقدم تقريره فيه وللقاضي ان يستبدل به غيره اذا لم يقدم التقرير في الموعد المحدد له ولا يترتب على عدم تحديد الموعد أي بطلان . ولم يوجب المشرع اتباع شكل معين في تقرير الخبير فقد يكون شفهياً او كتابة وفقاً لما تحدده طبيعة المهمة، ولكن الواقع العملي أثبت ان مايتم في الغالب الاعم هو ان يطلب من الخبير تقديم تقريره كتابة وخاصة اذا ما كانت المسألة موضوع الخبرة تتطلب إجراء ابحاث وتجارب وفحوصات علمية

[118] لم يعد هنالك خبراء جدول بصر فنظام خبراء الجدول اصبح الان جزء من التاريخ ولكن مازال يعمل بنظام خبراء الجدول في العديد من الدول العربية كما في دولة الامارات – بجانب الخبراء المعيين بوازة العدل او وزارة الداخلية

[119] امال عثمان –الخبرة في المسألة الجنائية رسالة دكتوراة كلية الحقوق جامعة القاهرة 1964م ص 416

ومعملية كما في قضايا التزيف والتزوير والطب الشرعي كقضايا القتل والإصابة والكيمياء الشرعية كقضايا السموم والمخدرات بل وغالباً مايرفق ملحقاً بالتقرير إيضاحياً مصوراً حتي يسهل على جهة التحقيق أو جهة الحكم تكوين عقيدتها و إقتناعها الذاتي بالدليل الفني في المسألة موضوع الخبرة .

و إذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية ، فإن أهمية إعداد تقارير فنية مكتوبة وملاحق توضيحة مصورة تصبح حتمية في حالة الجرائم المعلوماتية او الرقمية حيث يقتضي الأمر عرض وتوضيح وتحليل الدليل الجنائي الرقمي وكيفية إشتقاقه . [120]

حق الخصوم في رد الخبير

يحق للخصوم في شأن تنظيم الخبرة امام المحاكم – رد الخبير اذا وجدت أسباب قوية تدعو لذلك ويقوم طلب الرد الي المحقق للفصل ويجب ان يتبين فيه أسباب الرد وعلى المحقق الفصل فيه ويترتب على مجرد تقديم الطلب عدم استمرار الخبير فى عمله إلا في حاله الاستعجال وبأمر من المحقق.

نطاق الرأي الفني للخبير

ينصرف رأي الخبير الي الوقائع اللازم إصدار رأيه الفني بشأنه ، كما يجب أن يتوقف رأي الخبير عند حد إبداء رأيه الفني ولايتعدى الي غير المهمة الموكلة اليه ولايحق له التطرق الي أي مسائل قانونية أو غير قانونية . [121]

---

[120] الطعن رقم 4739 لسنة 56 ق جلسة 15|5|1997م مجموعة الاحكام ص 932
[121] جودة حسين جهاد –الوجيز في شرح قانون الاجراءات الجنائية لدولة الامارات العربية المتحدة مرحع سابق ص 375

وقد اعتنقت ذلك الرأي محكمة النقض المصرية في وضوح زجلاء حيث حكمت بأنه (...للمحكمة من توفير نيه القتل إذ إن دوره قاصر على إبداء رأيه الفني في وصف الاصابات وبسبب القتل ... [122]

وأخيراً فإن رأي الخبراء ماهو إلا أحد الادلة الجنائية التي تملك المحكمة حيالها التقدير وهذا الرأي مطروح أيضاً للمناقشة من كافة خصوم الدعوى إيراداً ورداً.

الإستعانة بخبير إستشاري للمتهم ان يستعين بخبير استشاري ويطلب تمكنه من الاطلاع على الاوراق على ان لا يترتب على ذلك تأخير السير في الدعوى وللخصوم رد الخبير إذا وجدت أسباب قوية تدعو لذلك ويقدم طلب الرد لقاضي التحقيق للفصل فيه ويجب أن تبين فيه أسباب الرد ،وعلى القاضي الفصل فيه.

مدى حجية تقرير الخبير :

الخبرة شأنها كشأن باقي أدلة الاثبات تخضع حجيتها لتقدير القاضي ومدى تأثير اعمال الخبرة في الاقتناع الذاتي للقاضي ، لما كانت المحكمة ملزمة بالإحالة الي رأي الخبرة الفنية وأخذ الرأي فيما يتعلق بمسألة فنية إلا إن محكمة الموضوع لها كامل السلطة في تقدير القوة التدليلية لعناصر الدعوى المطروحة على بساتط البحث وهى الخبير الاعلى في كل ما تسنطيع هي ان تفصل فيه بنفسها مادامت المسأله المطروحة ليست من المسائل الفنية البحته التي لا تستطيع المحكمة بنفسها أن تشق طريقها لإبداء الرأي فيها،فإن ما استخلصته المحكمة من مطالعتها للعقد موضوع الاتهام لا يحتاج الي خلرة تقديرية لأن إختلاف المواد يمكن تبينه بالعين المجردة [123].

---

[122] الطعن رقم 1354 لسنة 26 ق – جلسة 1957/1/14 مجموعة الاحكام ص 651

[123] الطعن رقم 145 لسنة 42 ق-جلسة 1972/1/24

وتجدر الاشارة الى انه وان كان من المقدر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير رأى الخبير الذى يرد عليها ، إلا ان ذلك لا يمتد الي المسائل الفنية إلا عن طريق خبرة فنية أخرى .

وأذا كان للمحكمة السلطة التقديرية في تقرير ما إذا كانت الادلة الموجودة في الدعوى كافية ويمكن الاستغناء بها عن تعيين الخبير من عدمه إلا أن ذلك مشروط بأن لا تتعرض للمسائل الفنية البحته التي تكون في نطاق دفاع المتهم[124] .

وقد قضت المحكمة العليا في إرساء حدود السلطة التقديرية لمحكمة الموضوع (...لايجوز للمحكمة ان تصنع نفسها محل الخبير الفني في مسألة فنية ، فإذا كان الحكم قد استند ،بين ما أستند اليه في ادانه المتهمين الي ان المجني عليه قد تكلم بعد اصابته وأفضى باسماء الجناة الي الشهود وكان الدفاع قد طعن في صحة رواية هولاء الشهود ونازع في قدرة المجنى عليه على التمييز والادراك بعد اصابته فإنه كان يتعين علي المحكمة ان تحقق عن طريق المختص فنياً وهو الطبيب الشرعي أما إذا لم تفعل ذلك فإن حكمها يكون معيباً لإخلالها بحق الدفاع مما يتعين معه الطعن ...).

وكذلك محكمة النقض المصرية في تقرير ذلك قضت بأنه ليس لمحكمة الموضوع أن تفصل في مسألة فنية دون أن تستعين بخبير فني يدلى بدلوه في تلك المسأله الفنية. [125]

ومن هذا نجد ان القضاء السوداني سار في ذات المنحى الذي سلكته محكمة النقض المصرية إلا إن المحكمة المصرية كانت أكثر تقيد اًلمحكمة الموضوع في سلطتها التقديرية حيث أجازت ان هي رأت أن تطرح رأي الخبير فعليها أن تستعين

---

[124]سعد حماد صالح القبائلي –حق المتهم في الاستعانة بمحام –مرجع سابق ص 89

[125]الطعن رقم 486 لسنة 34 ق –جلسة 1964/6/29- الطعن رقم 2397 لسنة 33 ق جلسة 1964/1/27 –المستشار سعيد شعلة ملاجع سابق ص 348

بخبير أخر وان يكون ذلك في نطاق من المنطق المقبول السائغ في حين ان القضاء السوداني أطلق العنان لمحكمة الموضوع في سلطتها عند تقديرها لأراء الخبراء وجعلها هي الخبير الاعلي حتى ولو كان الامر متعلقاً بمسألة فنية بحته ومن وجهة نظر المحكمة فلها ان تحيل الي اهل الخبرة وعليها ان تقدر رأيهم بعد ذلك وهو امر محل نظر .

يظهر الواقع العلمي ان القاضي غالباً مايسلم بما خلص اليه الخبير في تقريره ويبني حكمه على اساسه وهذا التصرف منطقي من القاضي فلا شك في ان رأي الخبير ورد في موضوع فني لا اختصاص للقاضي به وليس من شأن ثقافته او خبرته القضائية ان تتيح له الفصل فيه بالإضافة الي ذلك فهو الذي إنتدب الخبير و وثق فيه ورأى أنه مناسب لمهمته

ويرى الفقه المصري ضرورة إعطاء قوة الزامية لتقرير الخبير وذلك على اساس ان القاضي إذا رفض رأي الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية.[126]

المبحث الثالث : بينة الخبير في الجرائم الالكترونية

أن انتداب خبير أمام المحكمة للإدلاء برأيه الفني في المجال المطلوب يساعد المحكمة في بناء عقيدتها وتأسيس حكمها عليه لذلك لا بد أن تأخذ المحكمة حذرها في الأخذ ببينة أهل الخبرة في الجرائم المعلوماتية وغالباً ما يكون رأى الخبير في الجرائم المعلوماتية مأخوذ من محتويات الحاسوب مثل وجود الحساب وتسجيل الدخول من الحاسوب المضبوط كمعروضات أما إذا جاء رأى الخبير من خلال تتبع الخطوات التي قام بها المتهم في أطار ارتكابه الجريمة الالكترونية لا بد أن يكون رأى الخبير في هذه الحالة محل تمحيص لان به جانب من التخمين ومن الخطأ بناء

[126]امال عبدالرحيم عثمان –الخبلاة في المسائل الجنائية مرجع سابق ص 307 ومابعدها

الحكم على رأى الخبير الذي يدلى بشهادته أمام المحكمة التي مفادها على سبيل المثال (أنني ومن خلال تتبعي لتحرك المتهم في الشبكة العنكبوتية وقام بإنشاء حساب في موقع التواصل الاجتماعي وقام بإرسال طلبات صداقة وعلق على بوستات الأصدقاء وقام بإرسال طلبات صداقة) سرد ليس له أي أساس قانوني يتم بناءً علي خيال واسع وبناء الحكم عليه لا يعدو إلا أن يكون حكما على تخمينات وافتراضات وهذا الخبير هو عبارة عن سينارست إن جاز التعبير . عليه أما إذا جاءت بينة الخبير من واقع جهاز حاسوب أمام المحكمة كمعروضات تم الحصول عليه بإجراء قانوني صحيح ناتج عن تفتيش صحيح واعتراف من المتهم أو أثبات ملكيته للجهاز موضوع شهادة الخبرة فهنا يتغير الوضع وينظر إلى البينة باعتبارها رأى علمي مجرد وهو السبب الاساسى من تسميته خبير .

ومن الخطأ الاستعانة بآراء خبراء التخمينات والخيال فمعظم الخبراء في مجال تتبع الجريمة الالكترونية من خلال تحركات المتهم في مواقع التواصل الاجتماعي هى وفى كثير من الاحيان أن يكون الخبير قد وضع نفسه في مكان المتهم ويدلى بشهادته كما لو أنه كان مرتكباً للجريمة الالكترونية، فهنا يجب أن نلفت نظر المحاكم المختصة بالنظر في الجرائم المعلوماتية بعدم انتداب خبير بدون وجود جهاز حاسوب يتم استخراج الأدلة منه فأنة بغير جدوى ولا يبرح مكانه انه تخمين يعجب المستمع والشاكي ويدين المتهم بشده ثم إن هناك اعتبارات لابد أن توضع في الاعتبار في شخص الخبير في مجال الدليل الالكتروني وهو المؤهل العلمي الاكاديمى فلا يعتد بخبير لايحمل مؤهل علمي رفيع كشهادة الدكتوراه مثلا آو الماجستير هذا ليس إنقاصا في الشهادات الأقل درجة ولكن لان الأمر حساس ويتم بناء حكم قد يقضى بحبس حرية الأشخاص وان المجال ليس لديه قواعد إثباتيه

معلومة ونذكر أن التجارب وان كانت طويلة ولا يسندها مؤهل علمي تعتبر خبره فى المجالات المختلفة إلا في الجرائم المعلوماتية فينبغي مراعاة ذلك.

وكل محكمة تبنى حكمها على بينات الخبراء من خلال تتبع تحرك المتهم في الشبكة العنكبوتية يكون حكمها معيباً إن لم يكن خطأ فادح وغير موفق فالخبير في الجرائم المعلوماتية يجب أن يتحدث من جراء محتويات الحاسوب وليس من خلال التتبع في الشبكة.

بينة الهاكر أمام المحاكم:-

إذا انتدبت المحكمة أحد مرتكبي جرائم الحاسوب للشهادة أمامها كخبير يجب أن تأخذ علماً بأن شهادته وبينته التي يدلى بها لا تعدو أن تكون إلا وضع نفسه في مكان المتهم وينظر كما لو أنه يريد ارتكاب الجريمة الالكترونية، كيف سيتحرك في الخطوات لارتكاب الجريمة ويقوم بسرد حيثيات دقيقة متقمصاً شخصية المتهم ليخلص في النهاية إلى أن المتهم قد أرتكب الجريمة وهنا يكون حكم المحكمة معيباً.لذلك ننادى قضاة محكمة الموضوع الى عدم الاستعانة الا بشهود الخبرة بعد التاكد من مؤهلاتهم العلمية ، هذا بالاضافه الى عدم السماح للخبير بالتحدث بلسان المتهم.

بينة الشريك في الجرائم المعلوماتية:-

يعد الفرد شريكاً في جريمه:-

إذا كان لديه الدراية والعلم بالحدث، أي واقعة الجريمة، وكان قادراً على تبليغ الجريمة، ولكنه فشل في تحقيق ذلك مقصراً أو قاصداً. وبالتالي هذا الشريك يسمح للجاني بالاستمرار في تنفيذ جريمته بالرغم من أنه يمكنه منع الجاني إما عن طريق المنع المباشر، وإما بالاتصال مع السلطات، وقد يصبح هذا الفرد مساندا بعد ارتكاب الجريمة عوضاً من أنه متفرج بريء[127].

يحدد القانون مدى درجة الاشتراك في ارتكاب الجريمة. ولا تعتبر عادةً عملية الاشتراك جريمةً تلاحق قانونياً، بالرغم أنه أحياناً يتعارض مع المفهوم المتعارف لها وقد يصبح الشريك متامرا في الجريمة على حسب درجة تورطه، ماإذا اكتملت الجريمة أم لا.

يجعل مفهوم الاشتراك أو التواطؤمن الفرد مسئولاً من الناحية الجنائية جزاء أفعال الآخرين. وقد تشمل عملية الاشتراك في ارتكاب الجريمة مساندة الجاني والتآمر معه. وكثيراً ما يشار الي المسئولية لمساندة الجاني بالاشتراك في ارتكاب الجريمة .

يعد الشريك شريكاً في ارتكاب الجريمة، والاشتراك بنوعيه: إما بتورط الشريك من الدرجة الأولى في المشاركة الفعلية في ارتكاب الجريمة، وإما بتورط الشريك من الدرجة الثانية في المعاونة والتحريض فيه. وتكون المعاونة إما الجسدية وإما النفسية. ويسمى الشريك من الدرجة الثانية بالمتواطئ في ارتكاب الجريمة.

كما هو معلوم أن المحكمة يجب أن تأخذ ببينة الشريك في جرائم معروفة لغموضها ويتم عقد صفقة معه على أن يقوم بكشف غموض الجريمة وغالباً ما تكون من الجرائم الموجهة ضد الدولة والجرائم المخطط لها تخطيطاً دقيقاً والجرائم ذات الأدلة شبه المعدومة فيجب الأخذ ببينة الشريك في الجرائم المعلوماتية بحذر شديد لأن المتهم يكون قد سقط مرتين المرة الأولى حينما أرتكب الجريمة والثانية عندما أوشى بزملائه في الجريمة وهنا في جرائم الحاسوب الدخول إلى مواقع التواصل الاجتماعي

---

[127] معمر علي ابراهيم ، الادلة الالكترونية وحجيتها في الاثبات الجنائي – الطبعة الاولى 2014 مطبعة الخندق الخرطوم.

وإنشاء الحساب يشترط وجود كلمة سر وإذا كان الشريك لديه كلمة سر دخل بها أمام المحكمة وأنكر بقية المتهمين وهنا يوجد دليل غير بينة الشريك فمن الأوفق أن لا تبنى المحكمة حكمها على بينة الشريك في الجرائم الالكترونية والحكم على بقية المتهمين إذا كانت البينة الوحيدة ضدهم هي شهادة الشريك.

الدافع كبينة لارتكاب الجريمة الالكترونية:-

لو كان هناك متهماً بجريمة إلكترونية فليس للمحكمة الحق في اعتبار الدافع أحد دواعي ارتكاب الجريمة لأن أي شخص يستطيع أن يقوم بتسجيل حساب يوحى من خلاله بأنه شخص أخر خصوصاً إذا أراد أن يوقع شخص بعينه في جريمة إلكترونية،عليه فإن الدافع الشخصي الانتقامي في تقديري ليس من البينات المعتبرة لبناء عقيدة المحكمة والحكم على المتهم .

الدليل المستمد من كاميرات المراقبة:-

إن وضع كاميرات للمراقبة تعد مسألة ايجابية ومن شأنها أن تحد من ارتفاع الجريمة، سيما ما تعلق بمكافحة السرقة وتسجيل حيثيات حوادث المرور التي يتعمد مرتكبوها الهروب خشية العقاب، وتعد مثل هذه الإجراءات ، دليلا يثبت أطراف الجريمة في حالة تلبس، على غرار ما يحدث في الشركات التي تعتمد على كاميرات مراقبة وعليه تتمكن من رصد أي حركة تحدث في أروقتها وسيتم الاعتماد على التسجيلات في مختلف القضايا التي ستطرح على المحاكم وان الحرية الفردية محمية سيما وان هذه الكاميرات لن تقام داخل المنازل **أو** في أماكن دقيقة من شانها أن تضر بالمواطن ويمكن للمحاكم أن تبنى حكمها على الدليل المستمد من كاميرا المراقبة متى ما كان صحيحا تقنيا بعد مراجعته بواسطة خبير مختص وان كانت بعض التشريعات قد اختلفت في قبول الشريط المسجل بكاميرا المراقبة ولكن بعد

التقنيات التي تستطيع المحكمة من خلالها أن تطمئن على صحة الشريط يمكن أن يعتمد كدليل.

ان الشريط المسجل كبينة يمكن ان يستخدم في اثبات الجرائم ضمن ادلة اخرى ظرفية كانت او غيرها لتعضد بعضها بعضا وفي تقديري الجرائم المعاقب عليها بالاعدام او السجن المؤبد يجب ان تخذ المحكمة حذرها اذا كان الدليل المقدم ضد المتهم هو شريط مراقبة بالكاميرات.

اما انتهاك الخصوصية في المراقبة بالكاميرات في الاماكن العامة يجب الانتباه له جيدا فاذا كانت هناك ادلة مقدمة الى المحكمة بشريط مراقبة لاثبات جريمة يجب ان لا ينتهك هذا الشريط خصوصية الاخرين ليس لهم علاقة بالجريمة او الاثبات ويعامل من يظهر في الشريط معاملة التفتيش في الحاسوب فاذا كان تفتيش الحاسوب لاثبات جريمة معينة رغم الحصول على ادلة لجريمة اخرى او لافعال تشكل جريمة اخرى فيجب عدم الاخذ بالاثبات الغير مقصود والذي من اجله تم اجراء التفتيش لاثبات جريمة اخرى لم يكن قد تم فتح بلاغ مسبق بها للحفاظ على مبدأ عدم انتهاك خصوصية الغير.

الخاتمة

تتناول الخاتمة النتائج والتوصيات:

نظراً لما لوسائط الاتصالات من الانترنت وغيرها من أهمية بانت محلاً للكثير من الإعتداءات غير المشروعة التي اصبحت تشكل خطراً عليها ،ولخطورة هذه الظاهرة حاولنا في دراستنا هذه تسليط الضوء عليها .

سواء بالنسبة للإعتداءات الواقعة على حقول الانترنت ذاتها أو تلك الواقعة على أسماء النطاقات .

تتعدد اساليب وطرق الاعتداء على المواقع الا انها في مجملها تهدف الي مهاجمة هذه المواقع وتحقيق هدف معين للمهاجم من وراء ذلك وفي بعض الاحيان لا يكون هناك نفع للمهاجم سوى تعريض الموقع الضحيه للضرر، بتخريب نقطة الاتصال أو النظام وذلك بفتح مئات الألاف من الرسائل الالكترونية من جهاز الحاسوب الخاص بالمعتدى الى الموقع المستهدف حيث يؤدى ذلك الى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة فتنتقل الي جهاز

المعتدى ولعل من اخطر وسائل تدمير المواقع هو الفيروس المعلوماتي الذي يسبب دائماً خسائر فادحه وهذا مانسميه نحن بالارهاب الالكتروني .

من هنا كانت الدراسة لمعرفة كيفية مكافحة هذا الارهاب او الجرائم الالكترونية من ناحية عامة وأهم وسائل المكافحة بالضرورة معرفة الدليل الالكتروني الذي بموجبه يمكن محاكمة المعتدى محاكمة عادله .

ومسألة الدليل الالكتروني أصبحت مسألة شائكة تحتاج أولاً الى تدريب للمعرفة العلمية والعملية ، ثانياً ضرورة وجود تشريع لتحديد نوع الدليل المادى الذي قد يتم العثور عليه في الاجهزة الالكترونية أو أجهزة الحاسوب وتحديد أيضاً وزن أو قيمة الدليل في القوانين الجنائية المواكبه ومدى معرفة النيابة والشرطة والقضاء بهذه التقنية لذلك هذه الدراسة تنادى بتحديد نوع الدليل وإجراءات الوصول اليه قانونياً من حيث المشاهدة والمراقبة والتفتيش وشاهد الخبرة ودور الخبرة في ذلك ووزن البينة او شهادة الخبير في هذا المجال .

بتوفيق من الله تعالى تم جمع معلومات هذا البحث الذى لاشك انه يعتريه النقص ولكن حسبنا انه عمل بشرى والنقص فيه وارد مهما بذل الانسان من جهد وسعى ، لقد حاولت على مدار صفحاته ان أوضح بعض النقاط لكى نثرى بها ساحة البحث العلمى فأخذت فكرة مبسطة عن شبكة الانترنت واوضحت أهم وأخطر الجرائم الالكترونية وقصدنا بذلك جرائم الارهاب الالكتروني – وجرائم الانترنت الاخرى بصورة مبسطة ومن ثم خصصنا فصل كامل للدليل الالكتروني ومن ثم فصل أخر لمكافحة الجرائم الالكترونية محلياً ودولياً و تحدثنا عن الخبير في ذات المجال وصفاته ووزن بينته التي يقدمها أمام القضاء .

وخلال إعدادي لهذا البحث توصلت الي عدد من النتائج والتى هى إجابة عن تساؤلات البحث ، كما انه قد تبين لى بعض الأمور والقناعات التى تم طرحها في صورة توصيات .

أولاً : النتائج

1-لقد صاحب ظهور شبكة الانترنت وانتشارها الكبير والسريع ظهور العديد من المشاكل القانونية على الساحة ، وظهر مصطلح جديد عرف بأسم الفراغ القانوني لشبكة الانترنت .

2-كشف هذا النوع من الجرائم وإثباتها ليس بالشئ السهل وانما يستلزم استخدام تقنيات حديثة في عمليات التحرى والكشف عن الأدلة والتحقيق لأجل ذلك يمكن إستخراج تقنية المعلومات بشكل دائم كوسيلة من وسائل ضبط الجريمة والتحقق فيها .

3-ما من دول يمكنها النجاح في مواجهة هذه الانماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها في الدول سواء في مجال المساعدات القضائية المتبادلة أوفي مجال تسليم المجرمين أو في مجال التدريب.

4-إنشاء وحدة تحقيقات خاصة تتولى مهمة التحقيق في الجرائم المعلوماتية ومنها الجرائم المتعلقة بالنت والادعاء فيها والاهتمام بتدريب وتأهيل كوادرها بصورة مستمرة.

5-إيجاد قضاء متخصص مدرب للنظر في الجرائم المعلوماتية لحاجتها الخاصة التي قد لا تتوافرفي القضاء العادي .

6- تعزيز وتنشيط تبادل المعلومات بين اجهزة تنفيذ القانون من جهة وبين خبراء نظم المعلومات من جهة أخرى بهدف معرفة أبعاد الجرائم الالكترونية ومقدار الاضرار الناشئة عنها وسمات مجرميها وأساليب منع إرتكابها وملاحظة مرتكبيها .

7-وضع سياسة امنية محكمة لأجل المحافظة على أمن وسلامة وسرية المعلومات .

8-النظر للادلة المعلوماتية كأدلة أثبات من خلال أحكام المختصين في الجانب المعلوماتي ومن وجهة نظر قانونية (عمل مزدوج) .

9-العمل علي تفعيل الاتفاقيات الاقليمية والدولية للعمل علي مكافحة الجرائم الالكترونية والحد والسيطرة نوعاً ما عليها وخصوصاً الارهاب الالكتروني .

10- إتخاذ التدابير اللازمة لكل مشكلات الاختصاص القانوني والقضائى التي تثيرها الجرائم المتعلقة بشبكة الانترنت .

ثانيا: التوصيات

من خلال ما جاء فى هذه الدراسة اطرح التوصيات الاتية:-

1-التركيز على تنمية الوعى بالثقافة المعلوماتية وامن المعلومات والالمام بالخطر القادم الذى تخلفه اخطاء الثورة الرقميه وذلك للعاملين بالمؤسسات التى تعنى بهذا الشان وذلك من خلال عقد الدورات التدريبيه غير التقليديه والمحاضرات والندوات وورش العمل والمؤتمرات واستخدام كل الوسائل المتاحه لتحقيق ذلك لان مكافحة هذا النوع المستحدث من الجرائم يقتضى تأهيل وتدريب القائمين على هذه المكافحة .

2-وضع برامج حماية كافية من الاختراق والتدمير لمؤسسات الدوله الحيويه التى تستخدم التقنيات الحديثه والعمل على التحديث المستمر لهذه البرامج لتقوم بالتنبيه عند حدوث اى اختراق.

3-ضرورة اعداد واستقطاب الباحثين فى المجالات الامنيه والاجتماعيه .واستيعاب اشخاص ذوى خبره فى مجال التقنية.وتدريب العاملين بالمؤسسات المعنية(الشرطة–الامن –النيابة).وتطوير اجراءات الكشف عن الجريمة واثباتها خاصة فى مسرح الجريمة بحيث تتمكن من تقديم الدليل القاطع للجهات العدلية.

4-ضرورة التعاون بين الدول فى انشاء مراكز وطنية تهتم بقضايا الارهاب الالكترونى والجرائم الالكترونيه التى اكتسحت عالم الانترنت والتقنية ودراستها من النواحى التشريعيه وبيان اثرها السياسى والاقتصادى والاجتماعى .

5-العمل على مكافحة الجرائم الالكترونية دوليا على مستوى الاجراء الجنائى، بحيث يسمح بالاتصال المباشر بين اجهزة الشرطة فى الدول المختلفة وذلك بانشاء مكاتب متخصصة لجمع المعلومات عن مرتكبى الجرائم وتبادلها.

6-العمل على تعديل قانون الجرائم المعلوماتية الموجود بغرض توفير الحماية الجنائية ضد الجرائم الناشئة عن استخدام اجهزة الحاسوب وثورة المعلومات بصورة اشمل مما هى عليه الان،واستصحاب المعوقات التى صاحبت التطبيق القضائى فيما يتعلق بوسائل الاثبات واعطاءها الحجيه اللازمه.

7-تعديل قانون الاجراءات الجنائية لسنة 1991م بحيث يستوعب اجراءات التحرى والضبط الالكترونى والتفتيش الالكترونى ووسائله.

8-العمل على تعديل قانون الاثبات او اضافة باب فى قانون الاثبات يستوعب وسائل الاثبات الالكترونية واعطاءها الحجيه الكاملة ومساواتها بوسائل الاثبات التقليديه.

9-الاخذ بعين الاعتبار عند اعداد مثل هذه التشريعات لتامين تجانس التشريع الجديد وتناسقه مع النظام القانونى السائد فى الدولة والاسترشاد بقوانين الدول الاخرى والتزاوج والربط بين المسائل التقنية والمسائل القانونية واخراج قواعد قانونية وتقنية منسجمة ومترابطه مع ضرورة مراعاة الاشكاليات التشريعيه لتجنبها.

10- يجب العمل مع الجامعات والمراحل التعليمية الاخرى لدورها فى توعية الشباب والطلاب للحد من هذه الظاهرة والعمل من خلال المنابر الدعوية للحث على عدم السماح للشباب فى البيوت بقضاء ساعات طويله امام الحاسوب .

11- الإسراع بالانضمام الي الاتفاقيات الدولية الخاصة بمكافحة الجرائم الالكترونية الي جرائم الانترنت وخاصة المعاهدات الدولية لمكافحة الجرائم المعلوماتية والانترنت.

12- الاهتمام بالمؤسسات العلمية المتخصصة في مجال تقنية المعلومات لتكون مصدر دعم متكامل لمؤسسات الدوله القائمة على مكافحة الجرائم الالكترونية وإعداد أجهزة متخصصة للخبرة في مواجهتها.

قائمة المصادر والمراجع

أولاً : القرآن الكريم

ثانياً: السنة النبوية

ثالثاً: الكتب

كتب تفسير القران.

معاجم اللغة –مختار الصحاح.

القانون الجنائى 1991م .

الشبكة العنكبوتية .

أ/ المراجع باللغة العربية

1-السيد محمد الحسن شريف ،النظرية العامة للاثبات الجنائي دراسة مقارنة (القاهرة : دار النهضة ، 2002م)

2-العبيدي اسامة بن غانم ، التفتيش عن الدليل في الجرائم الالكترونية – المجلة العربية للدراسات الامنية المجلد29 العدد 58 نوفمبر-ديسمبر 2013

3-الفكى احمداى ، القانون الدولي لمكافحة الإرهاب الطبعه 1، القاهرة : دار النهضة ، ب ،ن)

4-أحمد فراج حسين، أدلة الإثبات في الفقه الإسلامي، ص 13، جرار كورنو معجم المصطلحات القانونية، 345/1.

5- احمد ضياء الدين محمد خليل-قواعد الاجراءات الجنائية ومبادئها في القانون المصري –مطبعة كلية الشرطة سنة 2004م

6-أحمد المهدي، أشرف الشافعي، التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها ط1، القاهرة، 2007،

7-حسين الغافري ، ومحمد الالفي ، جرائم الانترنت بين الشريعة الاسلامية والقانون، دار النهضة العربية ، 2008م

8-حسنين المحمدي بوادي، إرهاب الإنترنت، الخطر القادم، القاهرة : الدار الجامعية 2006م

9-خالد ممدوح ، فن التحقيق الجنائي في الجرائم الالكترونية ، (القاهره : دار الفكر الجامعي ، 2009م)

10- خالد المهيري-التحقيق الجنائي العلمي في الجريمة التقليدية والمعلوماتية – الطبعة الثانية – دار الكتب المصري الحديث القاهرة سنة 1992م

11- خبير فتح الله بصلة –حدود الاثبات العلمي في قضايا التزييف والتزوير – دراسة في المفاهيم والاساليب والاجراءات –دار نويار للطباعة – مصر – 2001م

12- سامي جاد عبد الرحمن واصل ، إرهاب ا لدولة في إطار القانون الدولي العام ، دار النهضة ، الطبعة الأولي ، 2004م

13- سراج الدين محمد الروبي ، ألية الانتربول في التعاون الشرطي ، القاهره : الدار المصرية اللبنانية ، 1998م

14- فرج علواني هليل، التحقيق الجنائي والتصرف فيه والادلة الجنائية، دار المطبوعات الجامعية ، الاسكندرية 2006

15- فاضل زيدان ، سلطة القاضى الجنائى فى تقدير الادله (ب ت)،(ب ن)

16- عبدالفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية – دار الكتب القانونية المحلة الكبرى 2007

17- عمر الفاروق الحسيني ، المشكلات الهامه في الجرائم المتصل بالحاسوب وابعادها الدولية ، دراسة تحليلية نقدية ،ط2 القاهرة 1995م

18- على زكي العرابي- المبادئ الاساسية للتحقيقات والاجراءات الجنائية- طبعه لجنة التليف والترجمة سنة 1940

19- عكاشة محمد عبد العال ، الانابه القضائية في نطاق العلاقات الخاصة الدولية ،(بيروت : الدار الجامعية ، 1992م)

20- محمد الامين البشري–التحقيق في الجرائم المستخدمة–الطبعة الاولي–جامعة نايف العربية للعلوم الامنية الرياض سنة 2004م

21- محمد زكي ابو عامر- الاثبات في المواد الجنائية- الفنية للطباعة والنشر – الاسكندرية- سنة 1985م

22- محمد فهمي –الموسوعة الشاملة لمصطلحات الحاسب الالكتروني –مطابع المكتب المصري الحديث–سنة 1991م
23- محمود مصطفى ، الاثبات في المواد الجنائية في القانون المقارن –الجزء الاول– النظرية العامة الطبعة الاولى – جامعة القاهرة 1978
24- مختار الصحاح ، للامام : محمد بن أبي بكر بن عبد القادر الرازي ، (القاهرة : مطبعة دار الجيل ، ب ، ن)
25- هشام محمد فريد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني ، بحث مقدم الي مؤتمر القانون والكمبيوتر والانترنت في مايو 2002م
26- هلالي عبدالله –التزام الشاهد بالعلام في الجرائم المعلوماتية دراسة مقارنة – دار النهضة العربية –القاهرة سنة 2000م
27- هيثم عبدالسلام محمد ، مفهوم الارهاب في الشريعة الاسلامية (لبنان : بيروت ، دار الكتب العلمية ، 2005)
28- يس عمر يوسف ، النظريه العامه للقانون الجنائي السوداني ، لسنة 1991، الدار الجامعية ،الطبعة الثانية ، 1996.

الرسائل العلمية ودوريات :

1-أسامة الكسواني ، التجسس الالكتروني وطرق مكافحته ، القاهرة : الدار الجامعية ، 2006م ،
2-المجلة العربية للدراسات الامنية والتدريب المجلد 28 العدد 56
3-اشرف دوية – المجموعة الدولية للمحاماة – طعن رقم (2040) مجموعة المكتب الفني – مصر ج 42/1123
4-ايمن عبدالله فكري ، جرائم نظم معلومات دراسة مقارنة رسالة دكتوراه كلية الحقوق جامعة المنصور

5-ناصر ابراهيم محمد زكى-سلطة القاض الجنائي في تقدير الادلة جامعة الازهر كلية الشريعة والقانون 1987م.

6-جميل عبد الباقي الصغير ، الحاسب الالي كوسيلة لأثبات الجرائم ، بحث مقدم لمركز دراسات الشرطة ، أكاديمية مبارك للأمن 2009م

7-جوهر بنت عبدالعزيز ال سعود ، الجرائم الالكترونية ومكافحتها

8-منيرة بنت فهد الحمدان ،الحاسب اداة الدجريمة ووسيلة اكتشافها

9-نبيل عبدالمعم جاد – أسس التحقيق والبحث الجنائي العلمي

10- يونس خالد عرب (جرائم الحاسوب) دراسة مقارنة رسالة الماجستير 1994م

11- عبدالعال الديري – المركز العربي لابحاث الفضاء الالكتروني- بحث منشور في موقع المركز 2013/1/13

12- اضواء على الاثبات في الجرائم المعلوماتية – منتدى شئون قانونية – منتديات استارز تايمز

13- احمد ضياء الدين-مشروعية الدليل في المواد الجنائية رسالة دكتوراة كلية الحقوق جامعة عين شمس عام 1983م

14- علي حسن الطوالبة ، مفهوم جرائم الإرهاب في ضوء التشريعات العربية الحديثة ،مركز الإعلام الأمني .

15- عبدالحافظ عبدالهادي عابد –الاثبات الجنائي بالقرائن-رسالة دكتوراة القاهرة سنة 1989م

16- شريهان نشأت المنيري، (مقال) – مجلة الاهرام الالكترونية – دورية متخصصة في الشئون الدولية –عدد الثلاثاء 11 فبراير 2014

17- شبكة الحوار نت الاعلامية – ويكيبيديا الموسوعة الحرة – الشبكة العنكبوتية.

18- د.عمر محمد بن يونس-مذكرات في الاثبات الجنائي عبر الانترنت ندوة الدليل الرقمي

19- لواء د.نبيل عبدالمنعم جاد- جرائم الحاسب الالي-بحث منشور بندورة المواجهة الامنية للجرائم المعلوماتية مركز دعم اتخاذ القرارباقيادة العامة لشرطة دبي مطبعة بن دسمال -دبي سنة 2005م .

20- محمد عبيد سعيد سيف مشروعية الدليل في المجالين الجنائي والتأديبي دراسة مقارنة -رسالة دكتوراة في علوم الشرطة -مصر.

21- ممدوح عبدالحميد عبدالمطلب-البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الالي والانترنت .

22- يونس عرب -حجية الاثبات بامستخرجات الالكترونية في القضايا المصرفية

ملحق رقم (1)

مقترح اضافة باب الى قانون الإثبات للجرائم المعلوماتية

عملا بإحكام دستور جمهورية السودان الانتقالي لسنة 2005م أجاز المجلس الوطني ووقع رئيس الجمهورية القانون الاتى نصه:-

اسم القانون وبدء العمل به

المادة 1

اسم القانون

يسمى هذا القانون ، قانون الإثبات (تعديل) لسنة 2014م ويعمل به من تاريخ التوقيع عليه

المادة 2

يضاف هذا الباب كملحق إثبات بقانون الإثبات لسنة 1994م للجرائم والمعاملات الالكترونية.

(أ) في المادة (3) بعد البند (4) يضاف التعديل (5) الجديد الاتى .

(5) تطبق أحكام هذا القانون على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية والمسائل الالكترونية .

(ب) في المادة (4) تضاف كلمات وعبارات التفسير والتفاسير ألمقابله لها الاتيه:-

(ج)يضاف هذا الباب كملحق إثبات بقانون الإثبات لسنة 1994م للجرائم والمعاملات الالكترونية

المادة 3

(1) تطبق أحكام هذا القانون على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية 2007م إذا ارتكبت كليا آو جزئيا داخل آو خارج السودان أو امتد أثرها داخل السودان وسواء كان الفاعل أصليا أو شريكا أو محرضا على أن تكون تلك الجرائم معاقبا عليها خارج السودان مع مراعاة المبادئ ألعامه الواردة في قانون الإثبات لسنة 1994م.

(2) يطبق هذا القانون على الإثبات في المعاملات والمسائل الالكترونية.

(3) تسرى أحكام هذا القانون على ما لم يكن قد سمعت فيه البينة من الدعاوى.

المادة 4

استثناء

تستثنى الأدلة، التي أعدت قبل صدور هذا القانون، الأحكام المعمول بها في الوقت الذي أعد فيه الدليل ، أو كان ينبغي إعداده فيه.

المادة 5

- تفسير.
- في هذا القانون ، ما لم يقتض السياق معنى آخر :
- ما لم يقتضى السياق أي معنى آخر فإن :
- مزودو خدمة الإنترنت Internet Service Providers : (ISP)
- شركه تقوم بعمل التوصيلات اللازمة سواء سلكيا أو لا سلكيا لتوصيل خدمة الانترنت لمشتركيها مقابل رسوم وتزود الأفراد والشركات الأخرى بخدمات الانترنت برسوم.

1- الاتصالات (Telecommunication) :

هي أية وسيلة لإرسال أو استقبال الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أياً كان محتواها ، وسواء كان الاتصال سلكياً أو لاسلكيًّا بعد تحويلها رقميا في شكل إشارات إلكترونيه عبر قنوات اتصال سلكيا أو لا سلكيا.

2-المعلومات (Information):

يقصد بها أيه بيانات تتم معالجتها وتنتج منها معلومة أو معلومات توسع أو تزيد نطاق الفهم للبيانات الأولية التي تتعلق بالكائن أو الشيء.

3-البيانات (Data) :

يقصد بها أي حقائق أو بيانات تتعلق بكائن أو شيء تعكس ما يمكن تداوله حول الكائن أو الشيء وتساهم في تعريفه.

4- نظام المعلومات(Information System)

يقصد به مجموعة البرامج والأدوات والمعدات والقوى البشرية في هيكلية إدارية لإنتاج وتخزين ومعالجة البيانات .

شبكة المعلومات (Information Network)

يقصد بها أي ارتباط بين نظامين أو أكثر من نظم المعلومات لتبادل المعلومات أو نقلها

الموقع الإلكتروني(Website)

يقصد به مكان إتاحة المعلومات على شبكة المعلومات(الانترنت) من خلال عنوان محدد. وهو مجموعة صفحات مترابطة على شبكة المعلومات العالمية تمثل كيانا بذاته وتشكل موضوعا أو موضوعات محددة ذات صله .

5-الالتقاط(Capture)

- يقصد به مشاهدة البيانات أو المعلومات الواردة في أيه رسالة إلكترونية أو الحصول عليها (سماع-مشاهده-قراءه ....الخ).

6-وسائط المعلومات (Media Information)

يقصد بها أجهزة تقانة المعلومات والاتصال والتي يتم من خلالها تخزين ،معالجة، عرض آو نقل المعلومات الرقمية.

7-المحتوى:(Content)

يقصد به محتوى المادة الإلكترونية سواء كان هذا المحتوى نصا أو صوره أو صوتا أو فيديو وما في حكمه .

8-الدليل (Computer Directory) :

- يقصد به وحده تنظيميه في هيكل حفظ الملفات على الحاسوب لعمل هيكل هرمي للملفات وإعطائها أسماء لتنظيم المجلدات،مثل (مستنداتي) (صوري) الخ.

9-التوقيع الإلكتروني (Digital Signature):

هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام

والرموز الإلكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها الشهادة الرقمية.

10- العقد الإلكتروني(Electronic Contract):

هو العقد الذي يتم إبرامه عبر الانترنت - هو الاتفاق الذي يتم انعقاده بوسائل الكترونية ، كليا آو جزئيا .

11- القرص الصلب(Hard disk):

- هو الجزء المسؤول عن التخزين طويل الأمد للمعلومات حتى في حالة قطع التيار.

12- الذاكرة الخارجية(External Memory):

- هي المكان الذي يتم تخزين البيانات بداخله أما بشكل مؤقت أو بشكل دائم .

13- الجهاز الإلكتروني:

- هو جهاز قادر على استقبال البيانات ومعالجتها إلى معلومات ذات قيمه يخزنها في وسائط تخزين مختلفة وفى الغالب يكون قادراً على تبادل هذه المعلومات مع أجهزه أخرى أيا كان نوعه .

14- الذاكرة المؤقتة (Cache Memory):

-هي ذاكره خاصة ذات سرعه عاليه مصممه لتزود المعالج بالأوامر والمعلومات الأكثر طلبا من قبل المستخدم ويفقد المعلومات بانقطاع الكهرباء.

15- ذاكرة الوصول العشوائي ألرام(Ram) :

ذاكره مؤقتة وتعرف بذاكرة الوصول العشوائي.

16- القرص المضغوط (CD:Compact Disc)

- وسط صغير محمول دائري الشكل مصنوع من البوليمر المقولب ويستخدم لتسجيل الصوت والصورة والنص إلكترونيا وحفظهما واسترجاع الصوت والصورة والمعلومات الأخرى في شكلها الرقمي.

هو قرص بصري يستخدم لتخزين البيانات.

17- كرت ربط الشبكه (Network Interface Card) (NIC):

- هو واجهة الشبكة وهو يسمح بربط جهاز حاسوب بالشبكة.

18- المودم(Modem) :

هو الجهاز الوسيط الذي من خلاله يتم الاتصال بخدمة الانترنت - عبر شبكة الهاتف

19- السجل (Registry):

- هو عبارة عن قاعدة بيانات تستخدم لتخزين الإعدادات وتحتوى على إعدادات الأجهزة والبرامج والمستخدمين وتفصيلات الجهاز الإلكتروني.

20- البريد الإلكتروني(Email):

- هو وسيله لتبادل رسائل إلكترونية عبر الانترنت أو غيرها من شبكات حاسوبيه سواء كانت ملفات نصيه أو صور أو ملفات صوتيه أو غيرها .

21- عنوان البريد الإلكتروني (Email address):

هو عنوان افتراضي تصل إليه رسائل البريد الإلكتروني ويتألف عنوان البريد الإلكتروني من جزأين تفصلهما علامة @.

22- الحساب الإلكتروني (Account):

- هو منفذ يسمح لك عبره بالخضوع للتوثيق والحصول على الإذن لاستخدام خدمات الانترنت من خلال إسم المستخدم وكلمة المرور.

23- المضايقة (Bullying) :

- التحرش من خلال الأذى اللفظي أو التعليقات الجنسية والاعتداء الجسدي والكلام من قبل شخص أو أكثر من المضايقين.

24- ملف الكمبيوتر (Computer File):

- مجموعه من المعلومات ذات الصلة(وثائق،برامج ،الخ) مخزنه على الكمبيوتر تحت مسمى خاص بها .

25- حقوق النشر والتأليف (Copyright):

- مجموعه من الحقوق الحصريه تنظم استخدام فكره أو عمل أو معلومات.

26- مخترق (Hacker):

- برنامج يخترق سرية برامج أخرى ويتخلل نظام التشغيل .أو الشخص الذي يقوم ببرمجة هذا البرنامج.

27- سرقة الهوية (identity theft) :

- الحصول على البيانات الشخصية لشخص آخر بطريقه غير شرعيه واستخدامها بطريقه غير قانونية.

28- محتوى غير قانوني (Illegal Content) :

- محتوى على الإنترنت يصنف على أنه غير مشروع وفقا للتشريعات الوطنية في هذا الصدد.

29- الإنترنت (Internet):

- شبكة عالمية عامة مفتوحة للجميع تتألف من أجهزة كمبيوتر متصلة تتم من خلالها عمليات نقل وتبادل المعلومات.

30- وسيلة الاتصال بالانترنت (Internet Connection):

يشير إلى الارتباط الذي يمكن من خلاله للمستخدمين الاتصال بالانترنت-

31- البرمجيات الخبيثة (Malware):

برمجيات صممت لاختراق أنظمة الكمبيوتر أو إلحاق الضرر بها

32- التلاعب (Manipulation):

التغيير في صورة أو ملف أو رسم إيضاحي بطريقة واضحة أو غير واضحة.

33- كلمة المرور (Password):

كلمة المرور أو كلمة السر هي تشكيلة من الحروف الأبجدية والأرقام والرموز تمكن من يعرفها من الوصول أو استعمال مورد أو خدمة محمية.

34- البيانات الشخصية (Personal Data):

أية معلومات خاصة بشخص ما طبيعي أو اعتباري

35- التصيّد (Fishing):

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت.

(40) عطل (Failure)

تعطل، انهيار يجعل المورد غير متاح.

(41) جدار نارى(Firewall)

عتاد أو برمجيات تستخدم لعزل أو لتصفية البيانات وحماية بيئة المعلومات المرتبطة بالإنترنت.

(42) متسلل (Hack, hacker)

عملية دخول نظام بطريقة غير قانونية – شخص يدخل بغض النظر عن سبب الدخول إلى نظام شخص أخر بدون ترخيص وبصورة غير قانونية ويمكن أن يكون هذا الهجوم سلبياً أو إيجابياً.

(43) التسلل (Hacking)

سلسلة العمليات التي تستخدم لخرق نظام لتكنولوجيا المعلومات.

(44) برنامج تجسس (Spyware)

برنامج يرسل معلومات حساسة من كمبيوتر مصاب بالعدوى إلى المهاجم.

(45) حصان طروادة (Trojan horse)

برنامج خبيث مستور داخل برنامج قانوني وداخل في نظم بغرض اختطافها وذلك لعدة أسباب منها إفساد البيانات والبرامج وتعديلها وتدميرها أو التسبب في الأعطال أو التنصت.

المادة 6

الدخول المصرح به للمواقع يحدد بواسطة عنوان البريد الالكتروني أو المودم المستخدم في الانترنت أو باى طريقه أخرى يتم إعدادها بواسطة مزودي خدمة الانترنت أو اى خبير تعتمده المحكمة المختصة .ومن يسمح لغيره باستخدام منافذ الانترنت الخاصة به استخداما غير مشروع يكون كما لو انه استخدمها بنفسه .

المادة 7

مع مراعاة إحكام المادة (6) أعلاه إذا كان الإثبات الوحيد في الجريمة هو بيانات مشترك ولم يقم مزود الخدمة بتسجيل بيانات المشترك يتحمل مزود الخدمة اى أضرار تقع على الشاكي وتحكم بها المحكمة .

المادة 8

تعتبر الرسالة الالكترونية وسيلة من وسائل التعبير عن الإرادة المقبولة قانونا لإبداء الإيجاب والقبول بقصد إنشاء التزام تعاقدي. على أن تكون خاضعة للسلطة التقديرية للقاضي حسب الادله التي تعضدها . وعلى المحكمة التحقق من عدم وقوع أي تلاعب أو تحريف في الرسالة الإلكترونية.

المادة 9

يعتبر السجل الالكتروني والعقد الالكتروني والرسالة الالكترونية والتوقيع الالكتروني منتجا للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لإطرافها أو صلاحيتها في الإثبات.

المادة 10

المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك علي سبيل المثال لا الحصر تبادل البيانات الالكترونية أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي الفاكس لها الحجية الكاملة في الإثبات شانها شان ألكتابه التقليدية على دعامة ورقيه متى ما يكون حفظها قد تم في ظروف تضمن كمالها .

المادة 11

للمحرّر الإلكتروني صفة النسخة الأصلية، إذا توافرت فيه الشروط الآتية:

أ. أنْ تكون المعلومات الواردة به قابلة للحفظ والتخزين بحيث يمكن في أي وقت الرجوع إليها.

ب. أن يكون محفوظًا بالشكل الذي تمّ إنشاؤه أو إرساله أو تسلّمه أو بأي شكل يُسهّل دقّة المعلومات التي وردت به عند إنشائه أو تسلّمه.

ج. أن تدلّ المعلومات الواردة به على من أنشأه أو تسلَّمه وتاريخ ووقت إرساله وتسلّمه.

د. إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا.

المادة 12

تعتبر البينان الماخوذه من مسرح الجريمة الالكترونية ملزمه متى اتبعت فيها الخطوات التالية التي تودي إلى الحفاظ على مسرح الجريمة كما مايلي:

1. تصويرالكمبيوتروما قد يتصل به من أجهزة بدقَّة تامّة ،وأخذ صورة لأجزائه الخلفيّة وسائر ملحقاته،وطباعة نسخه ورقيه من ملفات معينه في ذات الوقت .

2. ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة، وعمل نسخه الكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع وبعد ذلك إعادة عمل نسخه تعمل من جهاز التخزين خارج الموقع للمراجعة.

3. إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.

4. عدم التسرُّع في نقل أي مادّة معلوماتيّة من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة.

5. إتباع كافة إجراءات تحريز الدليل المذكورة في التفتيش وفق ما جاء في قانون الإجراءات الجنائية لسنة 1991م من المادة (86) إلى المادة (95).

6. الاستعانة بالخبراء لاستخلاص الادله من الجهاز وتعتبر البصمات الالكترونية للاجهزه المضبوطة حجه مكمله ودليل متى ما عضدته أدله أخرى وذلك حسب تقدير المحكمة.

7. الأدلة الإلكترونية المحصلة من أجهزة الحاسب الآلي يجب ان تكون مقبولة كأدلة إثبات ما دامت وظائف الكمبيوتر المتولد عنه الدليل سليمه وكان القائم عليه تتوافر به الثقه والطمانينه .
8. ضبط الجهاز وازالة ملحقاته ومراجعة محتوياته خارج الموقع.
9. يجب ان يتم التفتيش بواسطة تيم مختص او فريق عمل كما يجب التقاط صور فوتغرافيه وتحديد مواقع اجهزة الحاسوب فى المكان . كما يجب ان يضم فريق التفتيش خبير مسرح جريمه عاديه مثل خبير البصمات وخلافه حسب مقتضى الحال .

ملحق رقم (2)

مشروع قانون جرائم المعلوماتية لسنة 2015م

ترتيب المواد

الفصل الأول

أحكام تمهيدية

1. **إسم القانون .**

2. تطبيق

3. تفسير .

4- تسجيل هوية الاجهزة

5- ملحق اثبات

الفصل الثانى

جرائم نظم ووسائط وشبكات المعلومات

4. دخول المواقع وأنظمة المعلومات المملوكة للغير .

5. دخول المواقع وأنظمة المعلومات من موظف عام .

6. التنصت أو إلتقاط أو إعتراض الرسائل .

7. جريمة دخول المواقع عمداً بقصد الحصول على بيانات أو معلومات أمنية.

8. إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات .

9. إعاقة أو تشويش أو تعطيل الوصول للخدمة .

10. إستغلال المواقع أو الشبكات المملوكة للغير

11. إنشاء او إدارة أو تشغيل مواقع أو شبكات أو القيام بأي نشاط معلوماتي دون الحصول علي إذن أو تصديق مسبق من الجهات المختصة.

الفصل الثالث

الجرائم الواقعة على الأموال والبيانات والاتصالات

القيام باي عمل أو نشاط معلوماتي مناف للقانون بغرض الإحتيال علي الأموال أو البيانات أو الشبكات المملوكة للغير

10. التهديد أو الابتزاز .

11. الاحتيال أو انتحال صفة غير صحيحة .

12. الحصول على أرقام أو بيانات بطاقات الإئتمان .

13. الإنتفاع دون وجه حق بخدمات الإتصال .

- **جرائم الاحتيال وسرقة الرصيد**
- **الترويج لجرائم لعب الميسر والمقامره**

الفصل الرابع

جرائم النظام العام والآداب

14. الاخلال بالنظام العام والآداب .

15. إنشاء أو نشر المواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام أو الآداب .

16. انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة .

17. إشانة السمعة .

- **نشر وترويج الصور والفيديوهات وتلفيقها**

الفصل الخامس

جرائم الإرهاب والملكية الفكرية

18. إنشاء أو نشر المواقع للجماعات الإرهابية .

19. جريمة نشر المصنفات الفكرية .

سرقة المؤلفات والتعدى بالنسخ

الفصل السادس

جرائم الإتجار فى الجنس البشرى والمخدرات وغسل الأموال

21.الإتجار فى الجنس البشرى .

22. الإتجار أو الترويج للمخدرات **والخمور** أو المؤثرات العقلية .

23. غسل الأموال .

الاتجار فى الاعضاء البشريه

الفصل السابع

أحكام عامة

23. التحريض أو الإتفاق أو الإشتراك .

24. الشروع .

25. المصادرة .

26. إبعاد الأجنبى .

الفصل الثامن

إجراءات تنفيذ القانون

27. إصدار القواعد .

28. المحكمة المختصة .

29. النيابة المختصة .

30. الشرطة المختصة .

الفصل التاسع

تسجيل هوية أجهزة الهاتف السيار المركزي C-EIR

31- نظام تسجيل هوية أجهزة الهاتف السيار المركزي C-EIR

32- تنظيم عمل المشروع من

33- إلزام الشركات بدعم تشغيل المشروع المستمر و المحافظه علي الخصوصية

34- ضبط جرائم طمس هوية الأجهزة

35- محاربة الإستنساخ و بيع الأجهزة دون المواصفات و الأجهزة قصيرة العمر.

الفصل العاشر

إثبات للجرائم المعلوماتية

يضاف هذا الفصل كملحق إثبات بقانون جرائم المعلوماتية .

(5) تطبق أحكام هذا الملحق على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية والمسائل الالكترونية .

(1) تطبق أحكام هذا الملحق على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية 2015م إذا ارتكبت كليا آو جزئيا داخل آو خارج السودان أو امتد أثرها داخل السودان وسواء كان الفاعل أصليا أو شريكا أو محرضا على أن تكون تلك الجرائم معاقبا عليها خارج السودان مع مراعاة المبادئ ألعامه الواردة في قانون الإثبات لسنة 1994م.

(2) يطبق هذا الفصل على الإثبات في المعاملات والمسائل الالكترونية.

(3) تسرى أحكام هذا الفصل على ما لم يكن قد سمعت فيه البينة من الدعاوى.

بسم الله الرحمن الرحيم

مشروع قانون جرائم المعلوماتية لسنة 2015م

(.../... /2015م)

الفصل الأول

أحكام تمهيدية

إسم القانون .

1. يسمى هذا القانون " قانون جرائم المعلوماتية لسنة 2015م " .

تطبيق .

2. تطبق أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه إذا ارتكبت كلياً أو جزئياً داخل أو خارج السودان أو امتد أثرها **من أو إلي داخل** السودان وسواء كان الفاعل أصلياً أو شريكاً أو محرضاً على أن تكون تلك الجرائم معاقباً عليها خارج **أو داخل** السودان مع مراعاة المبادئ العامة الواردة في القانون الجنائي لسنة 1991 .

تفسير .

3. في هذا القانون ما لم يقتض السياق معنى آخر :

" **الإلتقاط** " يقصد به مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها،

" **البيانات أو المعلومات** " يقصد بها النصوص و الأرقام والحروف والرموز و كل ما يمكن تخزينه ومعالجته وتوليده وإنتاجه ونقله بالحاسوب أو أي وسائط الكترونية أخرى ،

"**شبكة المعلومات**" يقصد بها أي ارتباط بين أكثر من نظام معلومات للحصول على المعلومات أو تبادلها ،

" **المحتوى**" يقصد به محتوى المادة الالكترونية سواء كان ذلك المحتوى نصاً أو صورةً أو صوتاً أو فيديو وما في حكمها ،

" **المعلوماتية** " يقصد بها نظم وشبكات ووسائل المعلومات ، البرمجيات والحواسيب والانترنت والأنشطة المتعلقة بها ،

" **الموقع** " يقصد به مكان إتاحة المعلومات على شبكة المعلومات من خلال عنوان محدد ،

"**نظام المعلومات**" يقصد به مجموعة البرامج والأدوات والمعدات لإنتاج وتخزين ومعالجة البيانات أو المعلومات أو إدارة البيانات أو المعلومات ،

"**وسائط المعلومات**" يقصد بها أجهزة تقانة المعلومات والاتصال . **ومعدات وتراكيب وتطبيقات وبرمجيات تقانة المعلومات والاتصال وشبكات التوصيل**

الفصل الثانى

جرائم نظم ووسائط وشبكات المعلومات

دخول المواقع وأنظمة المعلومات المملوكة للغير .

4. كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً له ويقوم بدخول ذلك الموقع ولو كان مصرحا له بالدخول واستغل التصريح للحصول على معلومات لمصلحته او لمصلحة غيره او لتسبيب ضرر لغيره او لمجرد الدخول او ان يقوم ب:

(أ) بالإطلاع عليه أو نسخه يعاقب بالسجن مدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معاً

(ب) بإلغاء بيانات أو معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل استخدام عنوانه او قام بتسبيب ضررا للغير، يعاقب بالسجن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً .

(ج) يعاقب كل من يثبت دخوله الى اى موقع غير مصرح به حتى ولو لم يرتكب اى مما هو مذكور فى الفقرتين (أ) و(ب) يعاقب بنصف العقوبة .

دخول المواقع وأنظمة المعلومات من موظف عام .

كل موظف عام اوخاص ، يدخل بدون تفويض من الجهه المختصه موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير ولو كان مصرحا له بالدخول واستغل التصريح استغلالا ضارا، يعاقب بالسجن مدة لاتتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً.

التنصت أو إلتقاط أو إعتراض الرسائل .

كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها ، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً .

جريمة دخول المواقع عمداً بقصد الحصول على بيانـات أو معلومات أمنية .

كل من يدخل عمداً موقعاً أو نظاماً مباشرة أو عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب و ما في حكمها بغرض :

(أ) الحصول على بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً ،

(ب) إلغاء اوحذف اوتدمير اوتغييربيانات أو معلومات تمس الأمن القومي للبلاد أو الإقتصاد الوطني أو حذفها أو تدميرها أو تغييرها يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً .

إيقاف أو تعطيل أوإتلاف البرامج أو البيانات أو المعلومات .

كل من يدخل بأي وسيلة نظاماً أو وسائطاً أو شبكات المعلومات وما في حكمها ويقوم عمداً بإيقافها أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات أو مسحها أو حذفها أو إتلافها او مساعدة الغير اواستغلال تفويض ممنوح له فى ذلك ،يعاقب بالسجن مدة لا تتجاوز ست سنوات أو بالغرامة أو بالعقوبتين معاً

إعاقة أو تشويش أو تعطيل الوصول للخدمة .

كل من يعوق أو يشوش أو يعطل عمداً ، وبأي وسيله ، الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً .

الفصل الثالث

الجرائم الواقعة على الأموال والبيانات والاتصالات

التهديد أو الابتزاز .

كل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها في تهديد أو إبتزاز شخص آخر لحمله علي القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الإمتناع مشروعاً ، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً .

الاحتيال أو انتحال صفة غير صحيحة .

كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة ، بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند سوى ان كان ذلك الفعل بالداخل او الخارج ، او تزويد الغير ببرامج تسهل الاحتيال او يسبب لنفسه كسب غير مشروع او لغيره خساره غير مشروعه يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً .

الحصول على أرقام أو بيانات بطاقات الإئتمان .

كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول إلى أرقام أو بيانات للبطاقات الائتمانية وكل البطاقات المصرفيه أو مافى حكمها بقصد إستخدامها فى الحصول على بيانات الغير أو أمواله أو ما تتيحه تلك البيانات

أو الأرقام من خدمات او تزوير النقود الالكترونيه ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً

الإنتفاع دون وجه حق بخدمات الإتصال .

ماده غير واضحه كل من ينتفع دون وجه حق بخدمات الإتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً .

الفصل الرابع

جرائم النظام العام والآداب

الاخلال بالنظام العام والآداب .

كل من ينتج أو يعد أو يهيئ أو يرسل أو يخزن أو يروج او يساعد على انتاج او حيازة محتوى مخل بالاداب عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها،أي محتوى مخل بالحياء أو النظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً .

(2) كل من يوفر أو يسهل **او ينشر** عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها للوصول لمحتوى مخل بالحياء أو منافٍ للنظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً .

(3) إذا وجه الفعل المشار إليه في البندين (1) و(2) إلى حدث يعاقب مرتكبها بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً .

إنشاء أو نشر المواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام أو الآداب

كل من ينشئ أو ينشر أو يستخدم موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسوب أو ما فى حكمها لتسهيل أو ترويج برامج أو أفكار مخالفة للنظام العام أو الآداب داخل البلاد، يعاقب بالسجن مدة لا تتجاوز.ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً كما ينطبق على اى سودانى مقيم بالخارج.

انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة .

كل من ينتهك أو يسئ أي من المعتقدات الدينية أو حرمة الحياة الخاصة او يقوم بنشر صور او معلومات او بيانات او مستندات من غير موافقة اصحابها حتى ولو كانت شرعيه او افشاء اى معلومات ذات طابع شخصى او سرى من دون اذن اصحابهاعن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ، يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً.

إشانة السمعة .

كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لإشانة السمعة يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً.

الفصل الخامس

جرائم الإرهاب والملكية الفكرية

إنشاء أو نشر المواقع للجماعات الإرهابية.

كل من ينشئ أو ينشر أو يستخدم موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابيه تحت أي مسمي لتسهيل الإتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية . او تنفيذ عمليات

ارهابيه باستخدام الوسائل الالكترونية ،او التحريض على ارتكاب الجرائم بالوسائل المعلوماتية ، يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً **مراعاة ان ذلك موجود فى المواقع وايجاد طريقه لمعالجته فى اطار القانون الجنائى.**

جريمة نشر المصنفات الفكرية .

كل من ينشر دون وجه حق عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها أي مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها ما لم تكن متاحه عبر مواقع اخرى، وكل من يقوم بنشر المصنفات التى تم تسجيلها بموجب اى قانون سارى المفعول يعاقب بالسجن مدة لا تتجاوز سنة أو الغرامة أو بالعقوبتين معاً .

الفصل السادس

جرائم الإتجار فى الجنس البشرى والمخدرات

وغسل الأموال

الإتجار فى الجنس البشرى .

كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الإتجار فى الجنس البشرى أو تسهيل التعامل فيه او يشارك

فى عملية العرض والطلب ، يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً.

الإتجار أو الترويج للمخدرات أو المؤثرات العقلية .

كل من ينشئ أوينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الإتجار أو الترويج للمخدرات او ترويج الكحول أوالمؤثرات العقلية أو ما في حكمها أو يسهل التعامل فيها او يقوم بانشاء مواقع للمقامره بوسائل معلوماتيه ، يعاقب بالسجن مدة لا تتجاوز عشرين سنة أو بالغرامة أو بالعقوبتين معاً.

غسل الأموال .

كل من يقوم بعملية غسل الاموال بالتسهيل أو التحويل أو الترويج عن قصد أو إعادة تدويرها بواسطة شبكة المعلومات أو أحد أجهزة الحاسوب أو مافى حكمها ليكسبها الصفة القانونية مع علمه بأنها مستمدة من مصدر غير مشروع يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً .

الفصل السابع

أحكام عامة

التحريض أو الإتفاق أو الإشتراك .

يعد مرتكباً جريمة التحريض كل من حرض أو ساعد أو أتفق أو اشترك مع الغير على إرتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ، وإن لم تقع الجريمة يعاقب بنصف العقوبة المقررة لها .

(2) إذا وقعت الجريمة نتيجة لذلك التحريض يعاقب المحرض بذات العقوبة المقررة لها.

الشروع .

يعد مرتكباً جريمة الشروع كل من شرع فى إرتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون ويعاقب بنصف العقوبة المقررة لها .

المصادرة .

مع عدم الإخلال بحقوق الغير حسنى النية ، يجب على المحكمة في جميع الأحوال أن تحكم بمصادرة الأجهزة أو البرامج أو الوسائط المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها ، كما يجب إغلاق المحل أو المشروع الذي إرتكبت فيه أى من الجرائم الواردة فى هذا القانون إذا ما إرتكبت الجريمة بعلم مالكه ، وذلك للمدة التي تراها المحكمة مناسبة .

إبعاد الأجنبى .

بالإضافة إلى أي عقوبات منصوص عليها في هذا القانون أو أي قانون آخر ومع مراعاة نصوص الإتفاقيات الدولية يجب على المحكمة في حالة الجرائم المنصوص عليها في المواد 7 ،15 ، 16، 18 ، 20 ، 21 و 22 ، أن تحكم بإبعاد المدان إذا كان أجنبياً.

الفصل الثامن

إجراءات تنفيذ القانون

إصدار القواعد .

دون الإخلال بأحكام قانون الإجراءات الجنائية لسنة 1991 يجوز لرئيس القضاء أن يصدر قواعد خاصة لتحديد الإجراءات التي تتبع في محاكمة الجرائم المنصوص عليها في هذا القانون .

المحكمة المختصة .

ينشئ رئيس القضاء وفقاً لقانون الهيئة القضائية لسنة 1986 محكمة خاصة للجرائم المنصوص عليها في هذا القانون .

النيابة المختصة .

تنشأ بموجب أحكام قانون تنظيم وزارة العدل لسنة 1983 نيابة متخصصة لجرائم المعلوماتية .

الشرطة المختصة .

30. تنشأ بموجب أحكام قانون شرطة السودان لسنة 2008 شرطة متخصصة لجرائم المعلوماتية .

قانون رقم .... لسنة 2015 .

قانون رقم 13 لسنة 2007 .

الفصل التاسع

نظام تسجيل هوية أجهزة الهاتف السيار المركزي C-EIR

31- فى هذا الفصل ما لم يقتضى السياق معنى اخر فان كلمة:-

(1)بيانات المشترك:

بيانات خاصة بالمشترك (الافراد، جمعيات ومؤسسات) الذي يتلقى خدمة الاتصالات من المشغل.

(2) المشغل: شركة مساهمة تقدم خدمات الاتصالات الالكترونية او تشغيل البينة التحتية للاتصالات من خلال الاطار الممنوح للشركة.

(3) السلطة: هي سلطة خاصة بالاتصالات

(4) الهيئة : الهيئة القومية للاتصالات

(5) مسجل هوية الاجهزة: عبارة عن قاعدة بيانات لتعريف هوية اجهزة الهاتف السيار.

(6) مسجل هوية الاجهزة المركزي: قاعدة بيانات مركزية لتسجيل هوية الاجهزة.

(7) خدمات الرسائل القصيرة:

(8) الجهاز: هو جهاز او جزء من جهاز له علاقة مباشرة او غير مباشرة بشبكة الاتصالات الالكترونية او الرادوية.

(9) **IMEI** : الهوية الدولية للاجهزة.

32- المعلومات الخاصة ببيانات المشترك او معلومات الهوية الالكترونية يجب عدم استنساخها ، تغيرها ، توزيعها لاي غرض او استخدامها بدون اذن الهيئة.

33- مع عدم الإخلال بحقوق الغير حسنى النية ، يجب على المحكمة في جميع الأحوال أن تحكم بمصادرة

الاجهزة والمعدات والوسائل والادوات التي تم تغير هويتها ، والبرمجيات والادوات التي تم استخدامها لاجراء التغيرات ، انتاجها ، توزيعها ، ترويجها وشرائها .

-كل من يقوم بترويج الاجهزة الجديدة او المستعملة المخالفة للقوانين يعاقب بالسجن سته اشهر او بالغرامه او بالعقوبتين معا مع المصادرة او الابادة .

كل من يقوم بتقديم وثائق او معلومات غيرحقيقة فيما يتعلق بمعلومات الاشتراك للمشغل او وكيله لاستيفاء الاجراءات والمبادئ المتعلقة بالتسجيل والتى يتم تحديدها

بالوائح والقوانين الصادره من الهيئة يعاقب بالسجن مدة عام او الغرامه او العقوبتين معا.

36-اذا قام المشغل او وكيله من دون التأكد من الوثائق الضروريه للتسجيل بتكملة الاجراءات للمشترك يتحمل تعويض المضرور جراء هذا الاجراء اذا ثبت الضرر ويعاقب بالسجن مدة عام او الغرامه او العقوبيتين معا.

36- يجب على المشغلين عدم تقديم خدمة الاتصال للاجهزة المفقودة ، المهربة، المسروقه او الاجهزة التي تم تغيير هويتها الالكترونية في مسجل الاجهزة المركزي الموجود في الهيئة .

38- يجب على المشغلين تشغيل مسجل الاجهزة الخاص بهم بالتزامن مع مسجل الاجهزة المركزي الموجود في الهيئة لضمان منع الاجهزة غير القانونية التي تم توضيحها سابقا من الاتصال بشبكة الاتصالات للحرص على سلامه وفعالية البنيه التحتية ويتم ذلك خلال سته اشهر من تاريخ سريان هذا القانون .

39- كل من يقوم بتوصيل جهاز تم قطعه بموجب اجراءات صحيحه لاى سبب ان كان عبر مركز شكاوى الهيئه يعاقب بالسجن لمدة عام او بالغرامه او بالعقوبتين معا.

40- كل من يفشى سرية وأمن البيانات الخاصة بالمشتركين سواء كان موظفا في الهيئة أو بأحد مشغلي الشبكات يعاقب بالسجن سته اشهر ا و الغرامة أو بالعقوبتين معا.

الفصل العاشر

إثبات للجرائم المعلوماتية

41- يضاف هذا الباب كملحق إثبات بقانون الإثبات لسنة 1994م للجرائم والمعاملات الالكترونية .

(أ) في المادة (3) بعد البند (4) يضاف التعديل (5) الجديد الاتى .

(5) تطبق أحكام هذا القانون على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية والمسائل الالكترونية .

(ب) في المادة (4) تضاف كلمات وعبارات التفسير والتفاسير ألمقابله لها الاتيه:-

(ج)يضاف هذا الباب كملحق إثبات بقانون الإثبات لسنة 1994م للجرائم والمعاملات الالكترونية

تطبق أحكام هذا القانون على اى من الجرائم المنصوص عليها في قانون جرائم المعلوماتية 2007م إذا ارتكبت كليا آو جزئيا داخل آو خارج السودان أو امتد أثرها داخل السودان وسواء كان الفاعل أصليا أو شريكا أو محرضا على أن تكون تلك الجرائم معاقبا عليها خارج السودان مع مراعاة المبادئ ألعامه الواردة في قانون الإثبات لسنة 1994م.

(2) يطبق هذا القانون على الإثبات في المعاملات والمسائل الالكترونية.

(3) تسرى أحكام هذا القانون على ما لم يكن قد سمعت فيه البينة من الدعاوى.

43- تستثنى الأدلة، التي أعدت قبل صدور هذا القانون، الأحكام المعمول بها في الوقت الذي أعد فيه الدليل ، أو كان ينبغي إعداده فيه.

- في هذا القانون ، ما لم يقتض السياق معنى آخر :
- ما لم يقتضى السياق أي معنى آخر فإن :
- مزودو خدمة الإنترنت Internet Service Providers : (ISP)
- (مقدم خدمة الانترنت) يقصد به أى شخص أو منظمة توفر خدمة الانترنت مقابل رسم أو مجاناً
- شركه تقوم بعمل التوصيلات اللازمة سواء سلكيا أو لا سلكيا لتوصيل خدمة الانترنت لمشتركيها مقابل رسوم وتزود الأفراد والشركات الأخرى بخدمات الانترنت برسوم.

الاتصالات (Telecommunication) :

هي أية وسيلة لإرسال أو استقبال الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أياً كان محتواها ، وسواء كان الاتصال سلكياً أو لاسلكيًّا بعد تحويلها رقميا في شكل إشارات إلكترونيه عبر قنوات اتصال سلكيا أو لا سلكيا.

يقصد بها أى ارسال أو بث أو استقبال أى إشارات ، رموز ، نصوص ، صور ، اصوات ، أو معلومات بأى وسيله سلكية أو راديوية أو عبر الألياف الضوئية أو أى وسيله الكترونية أخرى.

4-المعلومات (Information):

يقصد بها أيه بيانات تتم معالجتها وتنتج منها معلومة أو معلومات توسع أو تزيد نطاق الفهم للبيانات الأولية التي تتعلق بالكائن أو الشيء.

5-البيانات (Data) :

يقصد بها أي حقائق أو بيانات تتعلق بكائن أو شيء تعكس ما يمكن تداوله حول الكائن أو الشيء وتساهم في تعريفه.

4- نظام المعلومات(Information System)

يقصد به مجموعة البرامج والأدوات والمعدات والقوى البشرية في هيكلية إدارية لإنتاج وتخزين ومعالجة البيانات .

شبكة المعلومات (Information Network)

يقصد بها أي ارتباط بين نظامين أو أكثر من نظم المعلومات لتبادل المعلومات أو نقلها

الموقع الإلكتروني (Website)

يقصد به مكان إتاحة المعلومات على شبكة المعلومات(الانترنت) من خلال عنوان محدد. وهو مجموعة صفحات مترابطة على شبكة المعلومات العالمية تمثل كيانا بذاته وتشكل موضوعا أو موضوعات محددة ذات صله .

37- الالتقاط (Capture)

يقصد به مشاهدة البيانات أو المعلومات الواردة في أيه رسالة إلكترونية أو الحصول عليها (سماع-مشاهده-قراءه ....الخ).

38- وسائط المعلومات (Media Information)

يقصد بها أجهزة تقانة المعلومات والاتصال والتي يتم من خلالها تخزين ،معالجة، عرض آو نقل المعلومات الرقمية.

39- المحتوى:(Content)

يقصد به محتوى المادة الإلكترونية سواء كان هذا المحتوى نصا أو صوره أو صوتا أو فيديو وما في حكمه .

40- الدليل (Computer Directory) :

يقصد به وحده تنظيميه في هيكل حفظ الملفات على الحاسوب لعمل هيكل هرمي للملفات وإعطائها أسماء لتنظيم المجلدات،مثل (مستنداتي) (صوري) الخ.

41- التوقيع الإلكتروني (Digital Signature):

هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام

والرموز الإلكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها الشهادة الرقمية.

العقد الإلكتروني(Electronic Contract):

هو العقد الذي يتم إبرامه عبر الانترنت - هو الاتفاق الذي يتم انعقاده بوسائل الكترونية ، كليا آو جزئيا .

42- القرص الصلب(Hard disk):

هو الجزء المسؤول عن التخزين طويل الأمد للمعلومات حتى في حالة قطع التيار.

43- الذاكرة الخارجية (External Memory):

هي المكان الذي يتم تخزين البيانات بداخله أما بشكل مؤقت أو بشكل دائم .

44- الجهاز الإلكتروني:

هو جهاز قادر على استقبال البيانات ومعالجتها إلى معلومات ذات قيمه يخزنها في وسائط تخزين مختلفة وفى الغالب يكون قادراً على تبادل هذه المعلومات مع أجهزه أخرى أيا كان نوعه .

45- الذاكرة المؤقتة (Cache Memory):

هي ذاكره خاصة ذات سرعه عاليه مصممه لتزود المعالج بالأوامر والمعلومات الأكثر طلبا من قبل المستخدم ويفقد المعلومات بانقطاع الكهرباء.

46- ذاكرة الوصول العشوائي ألرام(Ram) :

ذاكره مؤقتة وتعرف بذاكرة الوصول العشوائي.

47- القرص المضغوط (CD:Compact Disc)

وسط صغير محمول دائري الشكل مصنوع من البوليمر المقولب ويستخدم لتسجيل الصوت والصورة والنص إلكترونيا وحفظهما واسترجاع الصوت والصورة والمعلومات الأخرى في شكلها الرقمي.

هو قرص بصري يستخدم لتخزين البيانات.

48- كرت ربط الشبكه (Network Interface Card) (NIC):

- هو واجهة الشبكة وهو يسمح بربط جهاز حاسوب بالشبكة.

49- المودم(Modem) :

هو الجهاز الوسيط الذي من خلاله يتم الاتصال بخدمة الانترنت – عبر شبكة الهاتف.

50- السجل (Registry):

– هو عبارة عن قاعدة بيانات تستخدم لتخزين الإعدادات وتحتوى على إعدادات الأجهزة والبرامج والمستخدمين وتفصيلات الجهاز الإلكتروني.

51- البريد الإلكتروني(Email):

– هو وسيله لتبادل رسائل إلكترونية عبر الانترنت أو غيرها من شبكات حاسوبيه سواء كانت ملفات نصيه أو صور أو ملفات صوتيه أو غيرها .

52- عنوان البريد الإلكتروني (Email address):

هو عنوان افتراضي تصل إليه رسائل البريد الإلكتروني ويتألف عنوان البريد الإلكتروني من جزأين تفصلهما علامة @.

53- الحساب الإلكتروني (Account):

هو منفذ يسمح لك عبره بالخضوع للتوثيق والحصول على الإذن لاستخدام خدمات الانترنت من خلال إسم المستخدم وكلمة المرور.

54- المضايقة (Bullying) :

التحرش من خلال الأذى اللفظي أو التعليقات الجنسية والاعتداء الجسدي والكلام من قبل شخص أو أكثر من المضايقين.

55- ملف الكمبيوتر (Computer File):

مجموعه من المعلومات ذات الصلة(وثائق،برامج ،الخ) مخزنه على الكمبيوتر تحت مسمى خاص بها .

56- حقوق النشر والتأليف (Copyright):

مجموعه من الحقوق الحصريه تنظم استخدام فكره أو عمل أو معلومات.

57- مخترق (Hacker):

- برنامج يخترق سرية برامج أخرى ويتخلل نظام التشغيل .أو الشخص الذي يقوم ببرمجة هذا البرنامج.

58- سرقة الهوية (identity theft) :

الحصول على البيانات الشخصية لشخص آخر بطريقه غير شرعيه واستخدامها بطريقه غير قانونية.

59- محتوى غير قانوني (Illegal Content) :

محتوى على الإنترنت يصنف على أنه غير مشروع وفقا للتشريعات الوطنية في هذا الصدد.

60- الإنترنت (Internet):

شبكة عالمية عامة مفتوحة للجميع تتألف من أجهزة كمبيوتر متصلة تتم من خلالها عمليات نقل وتبادل المعلومات.

61- وسيلة الاتصال بالانترنت (Internet Connection):

يشير إلى الارتباط الذي يمكن من خلاله للمستخدمين الاتصال بالانترنت-

62- البرمجيات الخبيثة (Malware):

برمجيات صممت لاختراق أنظمة الكمبيوتر أو إلحاق الضرر بها

63- التلاعب (Manipulation):

التغيير في صورة أو ملف أو رسم إيضاحي بطريقة واضحة أو غير واضحة.

64- كلمة المرور (Password):

كلمة المرور أو كلمة السر هي تشكيلة من الحروف الأبجدية والأرقام والرموز تمكن من يعرفها من الوصول أو استعمال مورد أو خدمة محمية.

65- البيانات الشخصية (Personal Data):

أية معلومات خاصة بشخص ما طبيعي أو اعتباري

66- التصيّد (Fishing):

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت.

(40) عطل (Failure)

تعطل، انهيار يجعل المورد غير متاح.

(41) جدار نارى(Firewall)

عتاد أو برمجيات تستخدم لعزل أو لتصفية البيانات وحماية بيئة المعلومات المرتبطة بالإنترنت.

(42) متسلل (Hack, hacker)

عملية دخول نظام بطريقة غير قانونية – شخص يدخل بغض النظر عن سبب الدخول إلى نظام شخص أخر بدون ترخيص وبصورة غير قانونية ويمكن أن يكون هذا الهجوم سلبياً أو إيجابياً.

(43) التسلل (Hacking)

سلسلة العمليات التي تستخدم لخرق نظام لتكنولوجيا المعلومات.

(44) برنامج تجسس (Spyware)

برنامج يرسل معلومات حساسة من كمبيوتر مصاب بالعدوى إلى المهاجم.

(45) حصان طروادة (Trojan horse)

برنامج خبيث مستور داخل برنامج قانوني وداخل في نظم بغرض اختطافها وذلك لعدة أسباب منها إفساد البيانات والبرامج وتعديلها وتدميرها أو التسبب في الأعطال أو التنصت.

(46) البطاقه الائتمانيه:-

(47) برتكول :

يقصد به مجموعة القواعد الرسمية والمواصفات التي تصف كيفية ارسال البيانات عبر الشبكة

(48)الانترنت :

يقصد به مجموعة شبكات يوجد بينها توصيل بينى تستخدم برتكول الانترنت

(49)برتكول الانترنت:

يقصد به برتكول طبيعة الشبكة السائد ويستخدم مع برتكول التحكم في الارسال

الدخول المصرح به للمواقع يحدد بواسطة عنوان البريد الالكتروني أو المودم المستخدم في الانترنت أو باى طريقه أخرى يتم إعدادها بواسطة مزودي خدمة الانترنت أو اى خبير تعتمده المحكمة المختصة .ومن يسمح لغيره باستخدام منافذ الانترنت الخاصة به استخداما غير مشروع يكون كما لوانه استخدمها بنفسه ويمكن محاكمته على سبيل المسئوليه التقصيريه.

مع مراعاة إحكام المادة (6) أعلاه إذا كان الإثبات الوحيد في الجريمة هو بيانات مشترك ولم يقم مزود الخدمة بتسجيل بيانات المشترك يتحمل مزود الخدمة اى أضرار تقع على الشاكي وتحكم بها المحكمة .

-تعتبر الرسالة الالكترونية وسيلة من وسائل التعبير عن الإرادة المقبولة قانونا لإبداء الإيجاب والقبول بقصد إنشاء التزام تعاقدي. على أن تكون خاضعة للسلطة

التقديرية للقاضي حسب الادله التي تعضدها . وعلى المحكمة التحقق من عدم وقوع أي تلاعب أو تحريف في الرسالة الإلكترونية واى تشكيك معقول فى التلاعب بها يفسر فى مصلحة المتهم.

يعتبر السجل الالكتروني والعقد الالكتروني والرسالة الالكترونية والتوقيع الالكتروني منتجا للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لإطرافها أو صلاحيتها في الإثبات على ان تتحقق المحكمة من عدم التلاعب بها ويحق للمحكمة الاستعانه بالخبراء.

المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك علي سبيل المثال لا الحصر تبادل البيانات الالكترونية أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي الفاكس لها الحجية الكاملة في الإثبات شانها شان ألكتابه التقليدية على دعامة ورقيه متى ما يكون حفظها قد تم في ظروف تضمن كمالها

للمحرّر الإلكتروني صفة النسخة الأصلية، إذا توافرت فيه الشروط الآتية:

هـ. أنْ تكون المعلومات الواردة به قابلة للحفظ والتخزين بحيث يمكن في أي وقت الرجوع إليها.

و. أن يكون محفوظًا بالشكل الذي تمّ إنشاؤه أو إرساله أو تسلّمه أو بأي شكل يُسهّل دقّة المعلومات التي وردت به عند إنشائه أو تسلّمه.

ز. أن تدلّ المعلومات الواردة به على من أنشأه أو تسلَّمه وتاريخ ووقت إرساله وتسلّمه.

ح. إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا.

تعتبر البينان الماخوذه من مسرح الجريمة الالكترونية ملزمه متى اتبعت فيها الخطوات التالية التي تودي إلى الحفاظ على مسرح الجريمة كما مايلي:

تصويرالكمبيوتروما قد يتصل به من أجهزة بدقَّة تامّة ،وأخذ صورة لأجزائه الخلفيّة وسائر ملحقاته،وطباعة نسخه ورقيه من ملفات معينه في ذات الوقت واتباع الاجراءات التى يتم اتباعها فى مسرح الجريمة حسب نص قانون الاجراءات الجنائيه على ان تكون اجراءات التفتيش قد تمت حسب المعمول به فى القانون الجنائى السودانى.

إتباع كافة إجراءات تحريز الدليل المذكورة في التفتيش وفق ما جاء في قانون الإجراءات الجنائية لسنة 1991م من المادة (86) إلى المادة (95).

الاستعانة بالخبراء لاستخلاص الادله من الجهاز وتعتبر البصمات الالكترونية للاجهزه المضبوطة حجه مكمله ودليل متى ما عضدته أدله أخرى وذلك حسب تقدير المحكمة على ان تكون قد تمت بواسطة خبير البصمات المختص .

الأدلة الإلكترونية المحصلة من أجهزة الحاسب الآلي يجب ان تكون مقبولة كأدلة إثبات ما دامت وظائف الكمبيوتر المتولد عنه الدليل سليمه وكان القائم عليه تتوافر به الثقه والطمانينه.

ضبط الجهاز وازالة ملحقاته ومراجعة محتوياته خارج الموقع.

يجب ان يتم التفتيش بواسطة تيم مختص او فريق عمل كما يجب التقاط صور فوتغرافيه وتحديد مواقع اجهزة الحاسوب فى المكان . كما يجب ان يضم فريق التفتيش خبير مسرح جريمه عاديه مثل خبير البصمات وخلافه حسب مقتضى الحال ويعتبر الدليل الالكترونى المتحصل عليه بغير هذه الطريقه غير مقبول .